IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN, Plaintiff,	1:13-cv-307-EGB
V.	Senior Judge Eric G. Bruggink
UNITED STATES, Defendant.	July 6, 2020

AMENDED COMPLANT FOR REDUCED PLEADINGS

Plaintiff is seeking to have the "Stay" lifted in CFC Case No. 13-307C. A final decision on Plaintiff's petition was issued on 06/25/2020. Plaintiff is also seeking leave from this Court to file an Amended Complaint. Nine of the ten remaining infringement allegations reference the Plaintiff's Reissue Patent No. [RE43,891]. Plaintiff is seeking to drop the nine allegations relating to the '891 patent, and continue forward with the one remaining infringement allegation that reference Plaintiff's 7,385,497 ('497) patent. Plaintiff's '891 patent has been asserted in two pending cases: CAFC: Case No. 20-1508 (Infringement); and, S.C. District Court—Greenville: Case No. 6:20-cv-2270 (Antitrust Law Violation).

PARTIES

1. Plaintiff Larry Golden is a citizen of South Carolina and has a principal place of business at 740 Woodruff Road, #1102, Greenville, S.C. 29607.

2. The United States is the Defendant to this action based upon the actions and conduct of its agents, including at least the following agencies: Department of Homeland Security (DHS); Department of Homeland Security Science & Technology Directorate (DHS/S&T); Homeland Security Advanced Research Project Agency (HSARPA); and, National Aeronautics and Space Administration (NASA), and all other Government Agencies and personnel named in this pleadings.

JURISDICTION

3. The jurisdiction of this Court is based on the provisions of 28 U.S.C. § 1498(a). Under 28 U.S.C. §**1498**, whenever the **government** uses or manufactures an invention covered by a patent of the United States, without a license from the owner, the owner may only bring an action against the United States in the United States Court of Federal Claims.

4. This is a claim pursuant to 28 U.S.C. § 1498(a) for recovery of Plaintiff's reasonable and entire compensation for the unlicensed use or manufacture, for or by the United States, of inventions described in and covered by United States Patent Numbers: 7,385,497; 8,106,752; 9,096,189; 9,589,439; and, 10,163,287. Pending applications 16/350,683 and 16/350,874 are asserted in this complaint for claim construction and entry upon issue.

5. 28 U.S.C. § 1498(a): "Whenever an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner's remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture".

DESCRIPTION AND TECHNICAL RATIONAL OF A CMDC DEVICE

Plaintiff and Defendants' Communicating, Monitoring, Detecting, and Controlling (CMDC) Devices-------(Exhibit 1: CD Video of the DHS CMDC device)

6. The Plaintiff's communicating, monitoring, detecting, and controlling (CMDC) device is commercialized in the form of an improved cell phone, smartphone, smartwatch, laptop, or tablet. The specifications and capabilities of the CMDC devices that were developed for, manufactured and commercialized by third-party government contractors, Apple, Samsung, and LG, are significantly the same as the Plaintiff's CMDC device(s) as illustrated below:

- Communication: at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, cellular connection, long and/or short-range radio frequency (RF) connection, or GPS connection was "taken" for the benefit of the Government and for Government "use".
- Monitoring: at least one of a viewing screen for monitoring in real time, viewing screen monitoring for CBRNE-H signal alerts, viewing screen monitoring for CBRNE-H color coded indicator lights, or viewing screen monitoring for tracking, alerts, and heart rate.
- Detecting: at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor; that is wired or wireless, capable of being disposed within, on, upon or adjacent the CMDC device.
- Controlling: at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween, for sending signals to at least lock or unlock doors, stall, stop, or slowdown vehicles, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems.
- Central Processing Unit (CPU): is the programmable device capable of general-purpose computation. It is the engine of logic, as with the brain, and the core piece of hardware in the Patent Owner's CMDC device (i.e. communication devices, monitoring device; monitoring equipment). The Patent Owner's CPU is capable of arithmetic operations such as add and divide and flow control operations such as conditionals. The Patent

Owner's central processing unit (CPU) is the electronic circuitry within the CMDC device that executes instructions that make up a computer program.

- Biometrics: that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and or signature or a face recognition to at least gain access to the CMDC device or to prevent unauthorized use of the CMDC device.
- Lock, Unlock, Disabling Lock: the CMDC device being equipped to receive signals from or send signals to engage (lock), disengage (unlock), or disable (make unavailable) locks after a certain number of failed attempts to unlock.
- Near-Field Communication: Near Field Communication or NFC is a short-range communication channel. The purpose for this technology is to simplify first-time connections to other wireless technologies, like Wi-Fi and Bluetooth. Near Field Communication in a CMDC device can be used as part of a two-factor access control system for unlocking a door. Biometric Fingerprint recognition is used for authentication and NFC is used to transmit authentication information to a computer controlling the door. NFC is preferred over RFID because RFID has a frequency vulnerable for detonating bombs.
- Location and Tracking: The CMDC tracking is a process for identifying the location of the device, whether stationary or moving. Localization may be affected by a number of technologies, such as using multi literation of radio signals between (several) cell towers of the network and the device, or simply using GPS. Some GPS CMDC devices use wireless-assisted GPS to determine the user's location. In wireless-assisted systems, the device uses the orbiting GPS satellites in conjunction with information about the device's signal. Sometimes called enhanced GPS, wireless-assisted GPS can often get a fix on the user's location faster than a GPS-only receiver. Some wireless-assisted systems can work inside buildings, under dense foliage and in city areas where traditional receivers cannot receive signals. GPS-enabled CMDC devices with view screens can often display turn-by-turn directions as well as announce them through the device's speaker. A database of maps is used to provide the directions. The CMDC device locator provides GPS coordinates and can dial emergency CMDC device numbers. The

Government, parents and caregivers can track the device's location by device or online and can receive notification if it leaves a designated "safe area."

The communicating, monitoring, detecting, and controlling (CMDC) device is also referred to as a "communication device", "monitoring device", "monitoring equipment", "cell phone detection device", multi-sensor detection device", multi-sensor detection system", "cell phone", "smart phone", "desktop", "handheld", "personal digital assistant" (PDA), "laptop", "computer terminal", or "smartwatch", because all can be *grouped together by common features of design similarities.*

Defendants CMDC Devices	**Patent #: 10,163,287; Independent Claim 4, 5 & 6**	**Patent #: 9,589,439; Independent Claim 22 & 23**	**Patent #: 9,096,189; Independent Claim 1**	**Patent #: 8,106,752; Independent Claim 10**	**Patent #: 7,385,497; Independent Claim 1**
DHS; S&T "Cell-All" initiative. Develop CMDC device to detect deadly chemicals". Stephen Dennis; PM: Contracts to Qualcomm, LG, Apple, and Samsung. Sensors will integrate with 261 million CMDC devices (i.e. smartphones)	Claim 4: A communication device, comprising: Claim 5: A monitoring device, comprising: Claim 6: Monitoring equipment, comprising:	Claim 22: A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal, comprising: Claim 23: A cell phone comprising:	Claim 1: A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:	Claim 10: A multi-sensor detection and lock disabling system for monitoring products and for detecting explosive, nuclear, contraband, chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:	Claim 1: A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:

<u>THE DEFENDANT'S INCIDENTAL USE OF PLAINTIFF'S CLAIMED CMDC DEVICES</u>

7. The Government cannot claim "incidental use" of Plaintiff's CMDC devices when the Government accepted information describing the CMDC device from the Plaintiff; the Government appropriated funding for a CMDC device to the DHS and other government agencies; the DHS and other government agencies issued solicitations (i.e. request for proposals) for the development of a CMDC device (**Exhibit 2**: DHS *Cell-All* solicitation; **Exhibit 3**: Plaintiff's proposal in response to the *Cell-All* solicitation); the Government awards and funds third-party government contractors for research and development, manufacture, and commercialization of Plaintiff's CMDC devices (**Exhibits 4 & 5**: DHS *Cell-All* third-party government contractors); and, the Government continues to appropriated funding, issue solicitations, award and fund third-party government contractors for research and development, manufacture, and commercialization of Plaintiff's CMDC devices through various government agencies (**Exhibit 6**).

8. Use "for" the government can be present even where the "primary" beneficiary is a private party. *See Advanced Software*, 583 F.3d at 1378 (finding government use, despite the fact that the primary benefits accrued to private banks, because the use also served national interests (i.e. Apple, Samsung, and LG's CMDC devices that monitors and detects for CBRN&Es).

VIOLATION ALLEGED

Claim for Relief

(Violation of Section 28 U.S.C. § 1498(a): Government Infringement)

9. Plaintiffs incorporate and reallege, as through fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

10. Upon information and belief, the United States has infringed, and continues to infringe, at least claims 1 of the '497 Patent, claim 10 of the '752 Patent, claim 1 of the'189 Patent, claim 23 of the'439 Patent, and claim 5 of the '287 Patent, as a current manufacturer, consumer, and/or user of the "Cell-All": Synkera MikroKera Ultra: Synkera presented the MikroKera Ultra Module at the Department of Homeland Security S&T "Cell-All" demonstration in Los Angeles on September 28, 2011. Synkera offers a general-purpose digital module for evaluation and use of MikroKera Ultra chemical sensors. Synkera Technologies has been funded by DHS to develop sensors that are suitable for integration into cell phones and other ubiquitous electronic devices carried by first responders and the public at large. The DHS S&T "Cell-All" project goal is to develop sensors that can detect life-threatening gases to be incorporated into cell phones. One feature of the Synkera MikroKera Ultra is: available with or without case. The monitoring equipment for this "Cell-All" project is at least a Samsung Galaxy smartphone that has an Android operating system (O/S).

11. The Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), Cell-All aims "to equip your cell phone (e.g. Apple iPhone) with a sensor capable of detecting deadly chemicals", says Stephen Dennis, Cell-All's program manager. S&T pursued cooperative agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. Jing Li, a physical scientist at NASA's Ames Research Center, developed new technology that would bring compact, low-cost, low-power, high-speed nanosensor-based chemical sensing chip which consists of 64 nanosensors and plugs into an Apple iTouch 30-pin dock connector. The new device is able to detect and identify chemicals in the air using a "sample jet" and sends detection data to another phone (e.g. Apple iPhone) or a computer via telephone communication network or Wi-Fi.

12. As a result of contracts with the U.S. Department of Homeland Security (DHS), Synkera Technologies Inc., and NASA's Ames Research Center; cooperative agreements with LG Electronics, Apple Inc., and Samsung Electronics; the Government has development, manufacture, and commercialized a "*Cell-All*" CMDC device for the Government. The United States has funded the development of a "*Cell-All*" CMDC device to be used by or for the Government; authorized the use of the CMDC device for both its personnel and the public, without license or legal right, Plaintiff's claimed inventions of a CMDC device described in, and covered by at least that of Plaintiff's '497, '752, '189, '439 and '287 Patents (**Exhibit 7**: Amended Claim Chart)

ALL INDEPENDENT CLAIMS FOR THE PLAINTIFF'S '497, '752, '189, '439 & '287 PATENTS LISTED BELOW ARE AVAILABLE FOR CLAIM CONSTRUCTION

Pat. # 7,385,497	**Pat. # 8,106,752**	**Pat. # 9,096,189**	**Pat. # 9,589,439**	**Pat. # 10,163,287**	**App. # 16/350,683**	**Reissue App. # 16/350,874**
Claim 1 of the '497 Patent	Claim 10 of the '752 Patent	Claims 1, 2, 3, 4, 5, 6, 7, 8, & 9 of the '189 Patent	Claims 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, & 23 of the '439 Patent	Claims 1, 2, 3, 4, 5, & 6 of the '287 Patent	Claims 1 & 11 of the [683] Patent Application	Claims 13, 14, 15, 22, 23, 64, 74, 75, & 76 of the [874] Reissue Patent Application

PRAYER

WHEREFORE, Plaintiff respectfully requests judgment in its favor against the United States granting Plaintiff the following relief:

A. Entry of judgment that the inventions set forth in the '497, '752, '189, '439 and '287 patents have been used and manufactured by and for the United States without license or lawful right within the meaning of 28 U.S.C. § 1498(a);

B. Reasonable and entire compensation for the unlicensed use or manufacture by or for the United States, of patented devices covered by and described in the '497, '752, '189, '439 and '287 patents under 28 U.S.C. § 1498(a), in an amount to be determined at trial;

C. Plaintiff's reasonable fees for expert witnesses and attorneys, plus its costs in accordance with 28 U.S.C. § 1498(a);

D. Pre-judgment and post-judgment interest on Plaintiff's award; and

E. All such other relief that the Court deems just and proper.

Respectfully submitted,

s/ Larry Golden

Larry Golden
Plaintiff, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 6th day of July, 2020, a true and correct copy of the foregoing AMENDED COMPLANT FOR REDUCED PLEADINGS_was served upon the following defendant by Priority "Express" Mail:

David A. Foley, Jr.
Trial Attorney
Commercial Litigation Branch
Civil Division
Department of Justice
Washington, DC 20530
David.a.foley@usdoj.gov
202-307-0346

s/ Larry Golden

Larry Golden, Pro Se
740 Woodruff Rd., #1102
Greenville, South Carolina 29607
atpg-tech@charter.net

EXHIBIT 1

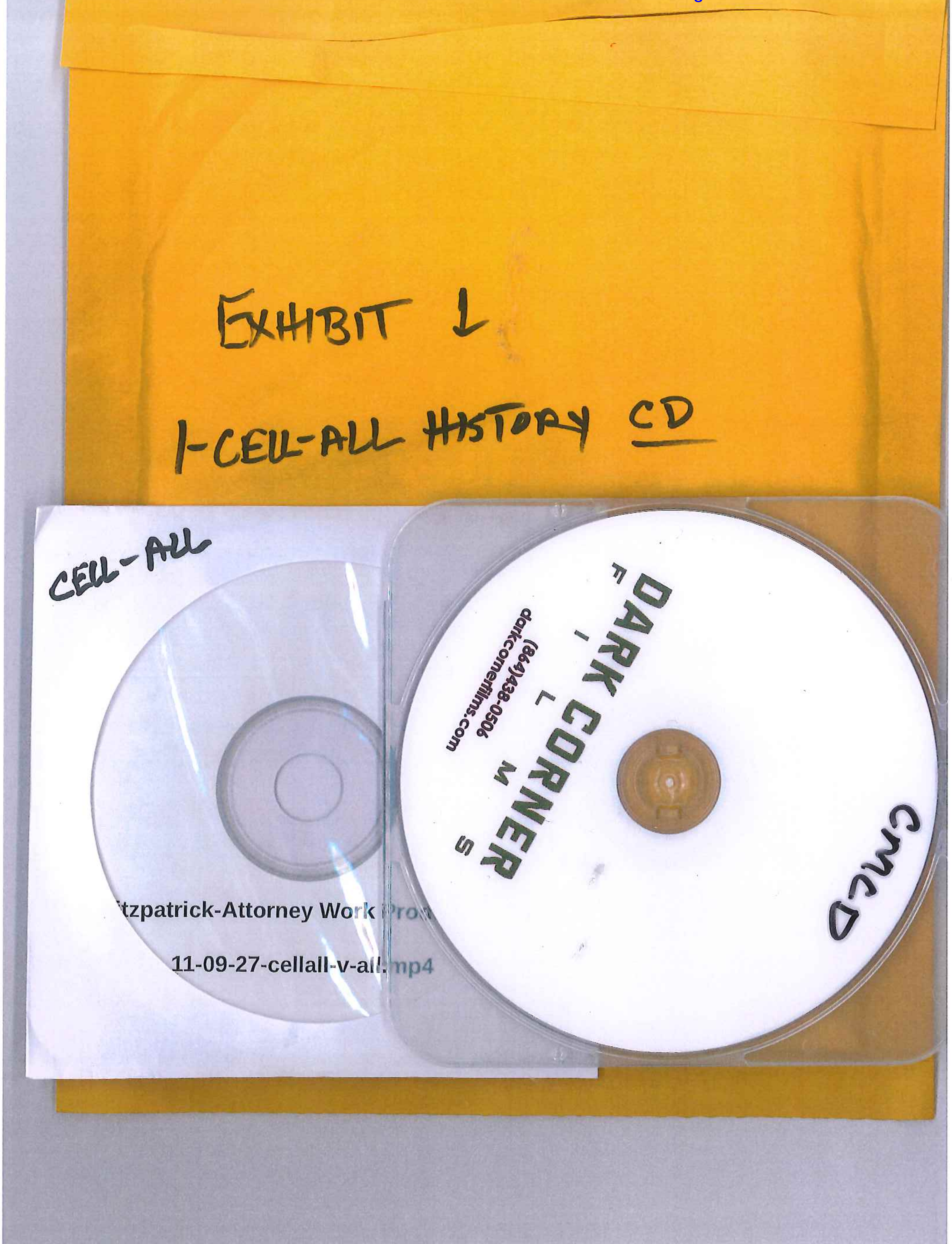


EXHIBIT 1
1-CELL-ALL HISTORY CD
CELL-ALL
tzpatrick-Attorney Work
11-09-27-cellall-v-al mp4
DARK CORNER
F I L M S
(864)438-0506
darkcornerfilms.com
CMCD

EXHIBIT 2

BROAD AGENCY ANNOUCEMENT (BAA)

BAA07-10

CELL-ALL Ubiquitous Biological and Chemical Sensing

Published: ***10/30/2007***

INTRODUCTION

This solicitation is a Broad Agency Announcement (BAA), as contemplated in Federal Acquisition Regulations (FAR) 6.102(d)(2) and 35.016. A formal Request for Proposal (RFP) will not be issued in this matter.

The Department of Homeland Security (DHS) Science & Technology (S&T) Directorate will not issue paper copies of this announcement. DHS S&T reserves the right to select for award and to fund all, some, or none of the full proposals received in response to this solicitation. No funding for direct reimbursement of proposal development costs will be allowed. Technical and cost proposals, or any other material, submitted in response to this BAA will not be returned. However, depending on the markings on the proposal, DHS S&T will adhere to FAR policy on handling source selection information and proprietary proposals. It is the policy of DHS S&T to treat all proposals as sensitive competitive information, and to disclose their contents only for the purpose of evaluation.

Awards may take the form of contracts or other transactions agreements (OTAs). In the event an offeror or subcontractor is a Federally Funded Research and Development Center (FFRDC), Department of Energy National Laboratory, or other Federally funded entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 U.S.C. 1531) or other appropriate authority. Depending on the nature of the full proposals received, DHS S&T will also consider awarding a grant or cooperative agreement. Therefore, the applicable laws and regulations governing the legal vehicle used for award will depend on the legal vehicle chosen by DHS S&T. In this regard, offerors should propose a preferred vehicle type for DHS S&T to consider for award.

I. GENERAL INFORMATION

1. Agency Name

Department of Homeland Security
Science & Technology Directorate
Washington, DC 20528

2. Research Opportunity Title

Ubiquitous Biological and Chemical Sensing

3. Program Name

CELL-ALL

4. Research Opportunity Number: BAA07-10

5. Important Dates

Event	Date	Time (local Eastern time)
White Paper Due Date	11/29/2007	4:30 P.M.
Notification of Evaluation of White Papers	12/14/2007	N/A
Full Proposal Due Date **(A Full Proposal will not be accepted unless a White Paper was received before the White Paper due date specified herein AND the Offeror was encouraged to submit a Full Proposal.)**	01/14/2008	4:30 P.M.
Notification of Evaluation of Full Proposals/Recommendation for Award	02/08/2008	N/A

* There is a registration process (see Section 4 of this BAA). A Prospective Offeror must ensure that it allow itself sufficient time to complete the registration and submission process. Extensions will NOT be granted.

Oral Presentations – Prospective Offerors are NOT provided the opportunity to make oral presentations.

6. Research Opportunity Description -

DHS S&T has designated this program as a High Impact Technology Solution (HITS), which is designed to a provide proof-of-concept answers within one to three years that could result in high-payoff technology (revolutionary) breakthrough. DHS S&T is seeking out those innovative, "out-of-box", possibly disruptive technologies (disrupting the normal evolutionary technological development process). It is recognized that this project will have considerable technological risk; however it also offers the potential for significant gains in capability. Innovation is critical. Offerors should demonstrate that their efforts are aimed at high-risk/high-payoff technologies that have the potential for making revolutionary rather than incremental improvements to homeland security, including emerging threats and operational challenges. ***DHS S&T reserves the right to select for award and fund all, some, or none of the Full Proposals received in response to this solicitation.***

Today's biological and chemical sensing networks work effectively to cover limited and specific physical areas and environments with significant cost and overhead. In order to greatly expand coverage and realize greater WMD protection for the nation, a revolutionary breakthrough that provides for a much larger and lower cost sensing distributed network is required. For example, if biological and chemical sensors could be effectively integrated into common cell phone devices and made available to the American public on a voluntary basis, the Nation could potentially benefit from a sensor network with more than 240M sensors. Through this BAA, HSARPA is seeking to accelerate advances in miniaturized biological and chemical sensing (e.g. laboratories on a chip) with integration into common

device(s) and a communication systems concept for large scale multi-sensor networks. This proof of concept should be capable of detecting hazardous biological and/or chemical materials with eventual expansion to the detection of explosive and eventually radiological materials (in future collaborations with other organizations). In the first year, proposed work should lead to a minimum of a relevant laboratory demonstration of a proof of concept sensor, device and communications system for Cell-All. Optional second year work may be proposed to build upon success in year one and may include additional field experiments and characterizations.

The proposed concept should develop a miniaturized sensor, device and system that when integrated is capable of addressing the following performance characteristics:

- Integrated into a common domestic platform, such as a cell phone
- User enabled so that the device can be switched on or off at the discretion of an individual user.
- Low cost and easy to maintain at scale
- Capable of accurately and securely communicating the location, date, time and binary outcome of sample readings
- Capable of receiving and displaying warning information from operations centers
- Demonstrates significant potential to provide accurate readings in a wide variety of environments
- Provides adequate sample collection methods within the host device to enable accurate sensing
- Provides sensing capability for multiple samples and any required methodology to readily refresh consumables
- Provides a reasonable power profile that does not significantly degrade the performance of the host device
- Survives a variety of environmental conditions
- Demonstrates an effective lifetime of more than one year.
- Supported by developmental architectures and development environments that promote low cost experiments, spiral prototyping and wide scale implementation

The contractor will also:

- Clearly define risks and vulnerabilities of the recommended technical approach and address methods to mitigate those risks and vulnerabilities
- Identify any barriers to ubiquitous sensing using the collection and sensor devices as proposed
- Provide a rough order of magnitude estimate of costs and overall schedule to develop each component and integrate into an overall system.
- List relevant experience in efforts that are similar

DHS S&T is receptive to individual or team offers. Technology developers must describe the schedule of incremental products they expect to produce.

7. Government Representatives

Science and Technology

Stephen Dennis
Program Manager
Department of Homeland Security
Science and Technology (S&T) Directorate
Washington DC, 20528

Business

Margaret L. "Margo" Graves
Team Lead/Contracting Officer
Department of Homeland Security
Office of Procurement Operations/Science & Technology Acquisitions Division
Washington, DC 20528

8. Catalog of Federal Domestic Assistance (CFDA) Number - 97.065

9. Catalog of Federal Domestic Assistance (CFDA) Title - Homeland Security Advanced Research Projects Agency

II. AWARD INFORMATION

Anticipated Award Information is as follows:

- Total Amount of Funding Available: **$3M** (subject to official fiscal appropriation)
- Anticipated Number of Awards: DHS S&T expects to make one or more awards.
- Anticipated Award Types: Anticipated to be in the form of a CPFF contract. However the Government reserves the right to award grants, Cooperative Agreements (CAs), or Other Transactions (OTs) Agreements to appropriate parties should the situation warrant use of a non-contractual instrument.
- Previous Year(s) Average Individual Award Amounts: N/A
- Anticipated Period of Performance for Award: 12 months. First year funding will be used to develop a proof-of-concept system for test and demonstration in the laboratory. Second year funding is optional and will be used to develop a prototype system and relevant field demonstration. Proposals that build on current or previous work are encouraged. If Offerors are extending work performed under other projects, it must clearly identify the point of departure and what existing work will be brought forward and what new effort will be performed under this BAA.

III. ELIGIBILITY INFORMATION

This BAA is open to **ALL** responsible sources.

Offerors may include single entities or teams from private-sector organizations, government laboratories, FFRDCs, including Department of Energy national laboratories and centers, and academic institutions.

Federally Funded Research & Development Centers (FFRDCs), are eligible to respond to this BAA, individually or as a team member of an eligible principal offeror, so long as they are permitted under a sponsoring agreement between the Government and the specific FFRDC.

Historically Black Colleges and Universities (HBCU), Minority Institutions (MI), Small Business concerns, Small Disadvantaged Business concerns, Women-Owned Small Business concerns, Veteran-Owned Small Business concerns, Service-Disabled Veteran-Owned Small Business concerns, and Historically Underutilized Business Zone (HUBZone) small businesses concerns are encouraged to submit proposals. They are also encouraged to join others as team members in submitting proposals. However, no portion of this BAA will be set-aside, pursuant to FAR Part 19.502-2.

Organizational Conflict of Interest

Organizational Conflict of Interest issues will be evaluated on a case-by-case basis; as outlined below. Offerors who have existing contract(s) to provide scientific, engineering, technical and/or administrative support directly to DHS S&T will receive particular scrutiny.

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more Offerors with the potential to attain an unfair competitive advantage.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the Offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the Offeror and include the appropriate provisions to mitigate or avoid such conflict in the contract awarded. After discussion with the Offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the Offeror may be found ineligible for award.

(c) Disclosure: The Offeror must represent, as part of its proposal and to the best of its knowledge that: (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract; or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation/Waiver. If an Offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the Offeror shall submit a mitigation plan to the Contracting Officer for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the Offeror. The Contracting Officer will use all information submitted by the Offeror, and any other relevant information known to DHS, to determine whether an award to the Offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful Offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

IV. APPLICATION AND SUBMISSION INFORMATION

1. Application and Submission Process

Oral Presentations – Prospective Offerors are **NOT** provided the opportunity to make oral presentations.

White Paper and Full Proposal submissions will not be accepted from organizations that have not registered; NO EXCEPTIONS. Any organization that wishes to participate in this solicitation must register at: http://www.hsarpabaa.com; before the due date and time established in this BAA; NO EXCEPTIONS. Therefore, a Prospective Offeror must ensure that it allow itself sufficient time to complete the registration process.

White Paper Process:

To begin the White Paper process, go to http://www.hsarpabaa.com, and select BAA07-10 from the list on the left side of the screen. Upon proper selection, buttons for registration and submission will appear. Select the appropriate registration button and fill in the requisite fields. Then submit your registration for White Paper submission.

Once the registration process is complete, registrants should receive a control identification number via e-mail. This control number is needed to begin the White Paper submission process. To submit your White Paper, select the appropriate submission button, fill out the requisite fields, upload your files, and then submit. Users will receive confirmation of their submission via e-mail. You may revise your White Paper submission up to the deadline for

receipt of White Papers. Failure to submit a White Paper will disqualify an Offeror from consideration for submitting a Full Proposal. NO EXCEPTIONS.

IMPORTANT NOTE: In teaming situations, the lead organization must remain the same on both the White Paper and, if encouraged, the Full Proposal. Any Full Proposal submitted by a organization that was not the lead organization for the White Paper submission will NOT be evaluated.

Full Proposal Process:

To begin the Full Proposal process (**ONLY those Offerors who are encouraged to submit a Full Proposal**), go to http://www.hsarpabaa.com, and select BAA07-10 from the list on the left side of the screen. Upon proper selection, buttons for registration and submission will appear. Select the appropriate registration button and fill in the requisite fields. Then submit your registration for Full Proposal submission.

Once the registration process is complete, registrants should receive a control identification number via e-mail. This control number is needed to begin the Full Proposal submission process. To submit your Full Proposal, select the appropriate submission button, fill out the requisite fields, upload your files, and then submit. Users will receive confirmation of their submission via e-mail. You may revise your Full Proposal submission up to the deadline for receipt of Full Proposals.

IMPORTANT: No Classified White Papers or Full Proposals (or portions of proposals) will be accepted.

White Paper and Full Proposal submissions will be protected from unauthorized disclosure in accordance with FAR 15.207, applicable law, and DHS regulations. Offerors are expected to appropriately mark each page of their submission that contains proprietary information.

The due date for White Papers is no later than 4:30 P.M. (Local Eastern Time) on **11/29/2007. White Papers WILL NOT BE ACCEPTED after the aforementioned date; NO EXCEPTIONS.** DHS S&T evaluation of the White Papers will be issued via e-mail notification on or about **12/14/2007**. Full Proposals will be subsequently encouraged from those offerors whose proposed technologies have been identified through the above e-mail as of "particular value" to DHS. However, any such encouragement does not assure a subsequent award. **A Full Proposal will not be accepted under this BAA unless a White Paper was received before the White Paper due date specified herein, AND the Offeror was encouraged to submit a Full Proposal.** Offerors submitting White Papers will not be debriefed. **THERE WILL BE NO EXCEPTIONS TO THIS RULE**. White Papers exceeding the page limit WILL NOT be evaluated; NO EXCEPTIONS.

The due date for receipt Full Proposals is 4:30 P.M. (Local Eastern Time) on **01/14/2008. Full Proposals WILL NOT BE ACCEPTED after the aforementioned date; NO EXCEPTIONS. A Full Proposal will not be accepted under this BAA unless a White**

Paper was received before the White Paper due date specified herein, AND the Offeror was encouraged to submit a Full Proposal. It is anticipated that award recommendations will be made on or before **02/08/2008.** As soon as the final proposal evaluation process is complete, each Full Proposal Offeror will be notified via e-mail as to whether or not its proposal has been recommended for award. Full Proposals exceeding the page limit WILL NOT be evaluated; NO EXCEPTIONS.

2. Format and Content of White Papers and Full Proposals

White Paper Format:

White papers may include narrative, pictures, figures, tables, and charts in a legible size, and must be accompanied by a one-page quad chart. Format details are:

- Paper Size – 8.5-by-11-inch paper
- Margins – 1 inch
- Spacing – Single- or double-spaced
- Font – Times New Roman, no smaller than 12 point. Text embedded within graphics or tables in the body of the white paper or the quad chart may not be smaller than 10 point.
- Number of Pages – No more than five single-sided pages, plus a one-page quad chart. Therefore, the entire mandatory white paper submission will not exceed ten (10) pages. Do not include a cover sheet (this is not the cover page discussed below), as one will be automatically generated for submitted white papers using the information provided during registration. If a cover sheet is submitted with the white paper, it will be counted toward the six-page white paper limit. White papers exceeding the page limit will not be evaluated.
- The White Paper shall consist of an electronic file in portable document format (PDF), readable by IBM-compatible personal computers (PCs). The quad chart must be submitted in the same file as the white paper. The file size must be no more than 10 megabytes (MB).
- Quad Chart Format – Quad charts will not use any font smaller than 12-point, except in graphics or tables, which may use 10-point fonts, and will be organized as follows:

<table>
<tr><td colspan="2">BAA Number: CELL-ALL BAA07-10
Title: *(Brief/Short Title to Describe Offeror's Proposed Effort)*</td><td>Offeror Name:
Date:</td></tr>
<tr><td>Photograph or artist's concept:
Provide a simple but sufficiently detailed graphic that will convey the main idea of the final capability and context for the concept and any prototype(s), and its technological methodology.</td><td colspan="2">Operational Capability:
1. *Performance targets*
2. *Quantify performance for key parameters*
3. *Cost of ownership*
4. *Address how the proposed development addresses the goals in the BAA.*</td></tr>
<tr><td>Proposed Technical Approach:
1. *Explain how it would meet and/or exceed the requirement/goals detailed in the BAA.*
2. *Describe tasks to be performed for base period.*
3. *Describe current status of the proposed technology.*
4. *Describe any actions done to date.*
5. *Describe any related ongoing effort by the offeror.*</td><td colspan="2">Schedule, Cost, Deliverables, & Contact Info:
Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option.
Deliverables:
Include all hardware, software and data deliverables.
Corporate Information:
You must include Offeror Name, POC full name, address, phone numbers and e-mail.</td></tr>
</table>

White Paper Content:

White papers should capture the essence of a proposal and are required for two purposes. First, they give the offeror an opportunity to obtain feedback from DHS S&T on their planned technology development without having to go to the expense and effort of writing a complete proposal. Second, the Government will evaluate the white papers as described in Section V to determine those submittals worthy of a full proposal. White papers shall be succinct and shall include, as a minimum, the following:

- Cover Page: The cover page (This is not the cover sheet previously discussed) shall be labeled "Proposal White Paper", and shall include the BAA number, proposed title, offeror's administrative and technical points of contact, with telephone numbers, facsimile numbers, and Internet addresses. An authorized officer will sign the cover page.

- Quad Chart: See template above.

- Executive Summary: Will contain a concise description of the scientific, technical, engineering, and management approach you propose to address the BAA, a

description of the various features of the proposed technology, and relevant details about how it will meet the Government's requirements.

- Utility to Department of Homeland Security: The white paper shall also describe the potential of the prototype for meeting the desired topic attributes and requirements given in BAA07-10.

- Technical Approach: Will contain a description of the basic scientific or technical concepts that comprise your proposed solution to the problem described in the BAA. Explain what is unique about your solution, and what advantages it might afford compared to other approaches that have been taken in this area. Illustrate the particular scientific, technical, or engineering issues that need to be addressed and resolved to demonstrate feasibility.

- Personnel and Performer Qualifications and Experience: Will briefly describe the offeror's qualifications and experience in similar development efforts. Present the qualifications of the principal technical team leaders. Describe the extent of your team's past experience in working with or developing the technologies comprising your solution.

- Commercialization Capabilities and Plan: Will provide a brief summary of the offeror's capabilities and experience in transitioning similar products to the marketplace, including previous business partnerships that can be leveraged. Describe the commercialization plan or other transition method for getting the technology into widespread use.

- Costs, Work, and Schedule: Will provide a brief summary of the planned work, costs, and schedule required to execute your project, summarized by task. Describe all required material, such as previously developed technology, test facilities, or other information which must be provided by the Government to support the proposed work.

- Small Business Considerations – If the prime Offeror is a large business, a commitment of the Offeror to the use of small business concerns.

Full Proposal Format:

Full proposals will consist of two volumes: a Technical volume and a Cost Proposal volume.

- Paper Size – 8.5-by-11-inch paper

- Margins – 1 inch

- Spacing – Single- or double-spaced

- Font – Times New Roman, 12 point. Text embedded within graphics or tables in the body of the white paper or the quad chart may not be smaller than 10 point.

- Number of Pages -
  - Volume 1: No more than **40** single-sided pages. Full proposals exceeding the page limit **WILL NOT** be evaluated. The cover page, table of contents, and resumes **are excluded** from the page limitations.
  - Volume 2: No page limitations.

- The Full Proposal shall consist of two electronic files (Volume 1 – Technical Proposal and Volume 2 – Cost Proposal) in portable document format (PDF), readable by IBM-compatible personal computers (PCs). The quad chart must be submitted in the same file as the white paper. The file size must be no more than 10 megabytes (MB).

<u>Full Proposal Content</u>

Volume 1: Technical Proposal

Volume I of the full proposal shall be in the form of a technical volume, not to exceed 40 pages, and a cost proposal overview. Responsiveness to the order and content of sections listed in Volume I is important to assure thorough and fair evaluation of proposals. The submission of other supporting materials with the proposal is strongly discouraged and, if submitted, will not be reviewed. Nonconforming proposals will be rejected without review.

The technical proposal shall cover all elements of the white paper. In particular, the technical proposal must cover the following points in more detail:

- <u>Cover Page (this is not the cover sheet previously discussed)</u>: This should include the words "Technical Proposal", and the following:

  1) BAA number
  2) Title of proposal
  3) Identity of prime offeror and complete list of subcontractors, if applicable
  4) Technical contact (name, address, phone/fax, e-mail address)
  5) Administrative/business contact (name, address, phone/fax, e-mail address)
  6) Duration of effort (separately identify the basic effort and any options)

- <u>Table of Contents</u>

- <u>Official Transmittal Letter</u>: This is an official transmittal letter with authorizing official signature. For electronic submission, the letter can be scanned into the electronic proposal. The letter of transmittal shall state whether this proposal has

been submitted to a government agency other than DHS and, if so, will specify which agency and the date it was submitted.

- Quad Chart: See example template in the box above.

- Executive Summary: This is a one-page synopsis of the entire proposal, including a listing of total anticipated costs. This page should include the proposal title and offeror name, along with a description of the scientific, technical, engineering, and management approach being proposed to address the goals of the BAA. It also should describe how the approach is unique, and provide a brief summary of the technology's anticipated performance. This section shall be separable, i.e., it will begin on a new page and the following section shall begin on a new page.

- Proposal: This describes the proposed work and the associated technical and management issues.

- Performance Goals: Describes the overall methodology and how it will meet the goals specified in the BAA.

- Detailed Technical Approach (no more than 15 pages): Describes the proposed design and technical issues. Identifies the critical technical issues in the design and concept. Identify technical risks in the approach and how they will be controlled a mitigated.

- Statement of Work (SOW), Schedule, and Milestones: Provides an integrated display for the proposed research, showing each task with major milestones. Include a section clearly marked as the SOW you propose to undertake. It is anticipated that the proposed SOW will be incorporated as an attachment to the resultant award instrument. To this end, such proposals must include a severable self-standing SOW without any proprietary restrictions, which can be attached to the contract or agreement award.

- Deliverables: Provide a brief summary of all deliverables proposed under this effort, including data, software, and reports consistent with the objectives of the work; along with suggested due dates (calendar days after the effective date of award). This section shall be severable, i.e., it will begin on a new page and the following section shall begin on a new page. It is anticipated that the proposed detailed list and description of all deliverables will be incorporated as an attachment to the resultant award instrument. To this end, such proposals must include a severable self-standing detailed list and description of all deliverables without any proprietary restrictions, which can be attached to the contract or agreement award.

- Management Plan: Provide a brief summary of the management plan, including an explicit description of what role each participant or team member will play in the project, and their past experience in technical areas related to this proposal.

- Commercialization Plan: Describe, in general terms, the offeror's capabilities and experience in transitioning similar products to the marketplace (including previous

business partnerships that can be leveraged), and specific plans for diffusion of technology developed via work proposed under this program. Describe a strategy for taking the proposed technology, if successful, from government-sponsored research and development to commercialization.

- Facilities: List the location(s) where the work will be performed, and the facilities to be used. Describe any specialized or unique facilities which directly affect the effort.

- Government-Furnished Resources: Provide a brief summary of required information and data which must be provided by the Government to support the proposed work, if any.

- Cost Summary: Summarize the projected total costs for each task in each year of the effort, including a summary of subcontracts, man hours, and consumables.

- Resumes for Key Personnel: In Appendix A, provide resumes and *curriculum vitae* (CVs) for each of the key personnel.

- Assertion of Data Rights: Include here a summary of any assertions to any technical data or computer software that will be developed or delivered under any resultant award. This includes any assertions to pre-existing results, prototypes, or systems supporting and/or necessary for the use of the research, results, and/or prototype. Any rights asserted in other parts of the proposal that would impact the rights in this section must be cross-referenced. If less than unlimited rights in any Data delivered under the resultant award are asserted, the Offeror must explain how these rights in the Data will affect its ability to deliver research data, subsystems and toolkits for integration as set forth below. Additionally, Offerors must explain how the program goals are achievable in light of these proprietary and/or restrictive limitations. If there are no claims of proprietary rights in pre-existing data, this section shall consist of a statement to that effect.

  Proposals submitted in response to this solicitation shall identify all technical data or computer software that the Offeror asserts will be furnished to the Government with restrictions on access, use, modification, reproduction, release, performance, display, or disclosure. Offeror's pre-award identification shall be submitted as an attachment to its offer and shall contain the following information:

  (1) Statement of Assertion. Include the following statement: "The Offeror asserts for itself, or the persons identified below, that the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose only the following technical data or computer software should be restricted:"

  (2) Identification of the technical data or computer software to be furnished with restrictions. For technical data (other than computer software

documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process as specifically as possible (e.g., by referencing specific sections of the proposal or specific technology or components). For computer software or computer software documentation, identify the software or documentation by specific name or module or item number.

(3) Detailed description of the asserted restrictions. For each of the technical data or computer software identified above in paragraph (2), identify the following information:

(i) Asserted rights. Identify the asserted rights for the technical data or computer software.

(ii) Copies of negotiated, commercial, and other non-standard licenses. Offeror shall attach to its offer for each listed item copies of all proposed negotiated license(s), Offeror's standard commercial license(s), and any other asserted restrictions other than government purpose rights; limited rights; restricted rights; rights under prior government contracts, including SBIR data rights for which the protection period has not expired; or government's minimum rights.

(iii) Specific basis for assertion. Identify the specific basis for the assertion. For example:

(A) Development at private expense, either exclusively or partially. For technical data, development refers to development of the item, component, or process to which the data pertains. For computer software, development refers to the development of the software. Indicate whether development was accomplished exclusively or partially at private expense.

(B) Rights under a prior government contract, including SBIR data rights for which the protection period has not expired.

(C) Standard commercial license customarily provided to the public.

(D) Negotiated license rights.

(iv) Entity asserting restrictions. Identify the corporation, partnership, individual, or other person, as appropriate, asserting the restrictions.

Previously delivered technical data or computer software. The Offeror shall identify the technical data or computer software that are identical or substantially similar to technical data or computer software that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or

subcontract. The Offeror need not identify commercial technical data or computer software delivered subject to a standard commercial license.

Estimated Cost of Development. The estimated cost of development for that technical data or computer software to be delivered with less than Unlimited Rights.

Supplemental information. When requested by the Contracting Officer, the Offeror shall provide sufficient information to enable the Contracting Officer to evaluate the Offeror's assertions. Sufficient information should include, but is not limited to, the following:

(1) The contract number under which the data or software were produced;

(2) The contract number under which, and the name and address of the organization to whom, the data or software were most recently delivered or will be delivered; and

(3) Identification of the expiration date for any limitations on the Government's rights to access, use, modify, reproduce, release, perform, display, or disclose the data or software, when applicable.

Ineligibility for award. An Offeror's failure to submit or complete the identifications and assertions required by this provision with its offer may render the offer ineligible for award.

This section shall be severable, i.e., it will begin on a new page and the following section shall begin on a new page. It is anticipated that the proposed Assertion of Data Rights will be incorporated as an attachment to the resultant award instrument. To this end, such proposals must include a severable self-standing Assertion of Data Rights without any proprietary restrictions, which can be attached to the contract or agreement award.

- Other DHS Support: As an appendix, provide a list of any current or pending awards or proposals with DHS. (This section will not count toward the 40-page limit).
- Small Business Considerations – If the prime Offeror is a large business, a commitment of the Offeror to the use of small business concerns.

Volume 2: Cost Proposal

The Cost Proposal shall consist of a cover page (this is not the cover sheet previously discussed) and two parts, Part 1 and Part 2. Part 1 will provide a detailed cost breakdown of all costs by cost category by calendar/fiscal year and Part 2 will cost breakdown by

task/sub-task using the same task numbers in the Statement of Work. Options must be separately priced.

Cover Page: The use of the SF 1411 is optional. The words "Cost Proposal" should appear on the cover page in addition to the following information:

- BAA number;
- Title of Proposal;
- Identity of prime Offeror and complete list of subcontractors, if applicable;
- Technical contact (name, address, phone/fax, electronic mail address)
- Administrative/business contact (name, address, phone/fax, electronic mail address) and;
- Duration of effort (separately price out the basic effort and any options)

Part 1: Detailed breakdown of all costs by cost category by calendar/fiscal year. The offeror should provide a total estimated price for major demonstrations and other activities associated with the program, including cost sharing, if any. The offeror should state whether any Independent Research and Development (IR&D) program is or will be dedicated to this effort, or if IR&D is being pursued to benefit related programs as well. Any cost sharing estimates should include the type of cost share, i.e. cash or in-kind. If in-kind is proposed, the offeror should provide a discussion of how the cost share was valued.

- Direct Labor – Individual labor category or person, with associated labor hours and ***unburdened*** direct labor rates;
- Indirect Costs – Fringe Benefits, Overhead, General & Administrative (Expenses), Cost of Money, etc. (***Must show base amount and rate***)
- Travel – Number of trips, destinations, durations, etc.
- Subcontract – A cost proposal ***as detailed as the Offeror's cost proposal*** will be required to be submitted by the subcontractor. The subcontractor's cost proposal can be provided in a sealed envelope with the Offeror's cost proposal or will be requested from the subcontractor at a later date;
- Consultant – Provide consultant agreement or other document which verifies the proposed loaded daily/hourly rate;
- Materials - Total direct material that will be acquired and/or consumed during the period of performance should be specifically itemized with costs or estimated costs. Where possible, indicate purchasing method, (Competition, engineering estimate, market survey, etc.). Limit this information to only major items of material (>$25,000) and how the estimated expense was derived. Include major facility requirements such as test ranges or live fire demonstrations. These requirements may address specific facilities, but should also provide details of facility capability requirements and estimates of total facility occupancy and test time. At its discretion, DHS(S&T) may choose to make bulk purchases of facility time in one or more major test facilities and apportion that test time to program participants.

- Other Directs Costs, particularly any proposed items of equipment or facilities. List the item, the estimated cost, and basis for the estimate. Equipment and facilities generally must be furnished by the contractor/recipient. Justifications must be provided when Government funding for such items is sought
- Fee/Profit including fee percentage.

Part 2: Cost breakdown by task/sub-task using the same task numbers in the Statement of Work.

The Cost Proposal should be consistent with your proposed SOW. Activities such as demonstrations required to reduce the various technical risks should be identified in the SOW and reflected in the Cost Proposal. The offeror should provide a total estimated price for the major Research, Development, Test, and Evaluation (RDT&E) activities associated with the program.

3. Significant Dates and Times

DHS S&T will review White Papers in accordance with the below anticipated schedule of events, using the evaluation criteria described above. After the White Paper review, DHS S&T will notify offerors, in writing, either encouraging or not encouraging submission of a Full Proposal based upon that review.

DHS S&T plans to review Full Proposals in accordance with the below anticipated schedule of events. A review panel will evaluate the Full Proposals using the criteria specified under the evaluation criteria discussed above. Following that review, offerors will be notified whether or not their proposal has been recommended for award. Multiple awards may be made under this BAA.

Event	Date	Time (local Eastern time)
White Paper Due Date	**11/29/2007**	4:30 P.M.
Notification of Evaluation of White Papers	12/14/2007	N/A
Full Proposal Due Date **(A Full Proposal will not be accepted unless a White Paper was received before the White Paper due date specified herein AND the Offeror was encouraged to submit a Full Proposal.)**	**01/14/2008**	4:30 P.M.
Notification of Evaluation of Full Proposals/Recommendation for Award	02/08/2008	N/A

* There is a registration process (see Section 4 of this BAA). A Prospective Offeror must ensure that it allow itself sufficient time to complete the registration and submission process. Extensions will NOT be granted.

The Government reserves the right to fund none, some, or all of the proposals received. It is the intention upon completion of proposal evaluation to notify offerors of an initiation of negotiation for awards or rejection of their proposal. Awards will be made based on the evaluation, funds availability, and other programmatic considerations.

4. Submission of Late White Papers and Full Proposals

White Papers and Full Proposals **WILL NOT BE ACCEPTED** after the published due dates and times. Extensions will **NOT** be granted.

5. Further Assistance Needed for this BAA

The applicable electronic address for "**ALL**" correspondence for this BAA is: BAA07-10@dhs.gov.

V. EVALUATION INFORMATION

1. Evaluation Criteria –

The following evaluation criteria apply to both the White Papers and the Full Proposals. The evaluation of White Papers and Full Proposals will be accomplished through an independent technical review of each; using the following criteria which is listed in descending order of importance. The sub-criteria listed under a particular criterion are of equal importance to each other.

A. The degree of innovation and potential to offer a revolutionary increase in capability or a significant reduction in cost commensurate with the potential risks of the innovative approach

B. Overall scientific and technical merits of the proposal
   1. The soundness of technical concept
   2. The Offeror's awareness of the state-of-the-art, future technology trends
   3. The Offeror's understanding of the scope of the problem and the technical effort needed to address it
   4. Intellectual Property Rights offered

C. Offeror's capabilities, related experience, and past performance, including the qualifications, capabilities and experience of the proposed principal investigator and personnel.
   1. The quality of technical personnel proposed;
   2. The Offeror's experience in relevant efforts with similar resources
   3. The ability to manage the proposed effort

D. Cost, including cost realism and reasonableness analyses. Each price/cost response will be reviewed for price/cost realism, reasonableness, and overall best

value to the government. Members of the Evaluation Team may presume that the technical approach provided by the Offeror serves as a rationale for the labor mix and labor hours used.

E. For proposed awards to be made as contracts to large businesses, the small business consideration section of each proposal will be evaluated based on the extent of the Offeror's commitment in providing meaningful subcontracting opportunities for small businesses, small disadvantaged businesses, woman-owned small businesses, HUBZone small businesses, veteran-owned small businesses, service disabled veteran-owned small businesses, historically black colleges and universities, and minority institutions.

The final evaluation will be based on an assessment of the overall best value to the government based on these criteria. Awards will be made based on proposal evaluation, funds availability, and other programmatic considerations, including awards to lesser rated proposals where orthogonal or alternate technologies are deemed to be more technically advantageous.

Industry-Academia Partnering – HSARPA highly encourages partnering among industry and academia with a view toward speeding the incorporation of new science and technology into fielded systems. Proposals that utilize industry-academic partnering which enhances the development of novel S&T advances will be given favorable consideration.

Industry-Government Partnering – HSARPA highly encourages partnering among industry and Government with a view toward speeding the incorporation of new science and technology into fielded systems. Proposals that utilize industry-Government partnering which enhances the development of novel DHS S&T advances will be given favorable consideration.

2. Evaluation Panel -

The evaluation of White Papers and Full Proposals will be performed by an Evaluation Team of government technical experts drawn from DHS and other Federal Government agencies.

The Government may use selected support contractor personnel to assist in the evaluation and administrative functions of any ensuing White Papers, presentations, and proposals from this announcement. These support contractors will be bound by appropriate non-disclosure agreements to protect proprietary and source-selection information and will not be permitted to release any source-selection information to third parties, including others in their organization.

VI. AWARD ADMINISTRATION INFORMATION

1. Administrative Requirements

- The North American Industry Classification System (NAICS) code for this announcement is 541710; with a small business size standard 500 employees.

- Central Contractor Registry (CCR)—Successful offerors not already registered in the CCR will be required to register in the CCR prior to award of any grant, contract, cooperative agreement, or other transaction agreement. Information regarding CCR registration is available at http://www.ccr.gov/.

- Certifications—In accordance with FAR 4.1201, prospective offerors for contracts, and other transaction agreements involving prototypes (Section 845), shall complete the Online Representations and Certifications Application (ORCA) at http://orca.bpn.gov. Offerors should make mention of its ORCA completion in its proposal, and provide its Certification Validity period. Successful offerors will be provided additional information with regards to certification for grants, cooperative agreements, or other transaction agreement (other than for prototypes) proposals.

- Subcontracting Plans - Successful contract proposals that exceed $650,000, submitted by all but small business concerns, will be required to submit a Small Business Subcontracting Plan in accordance with FAR 52.219-9, prior to award.

2. Objections

Any objections to the terms of this solicitation or to the conduct of receipt, evaluation, or award of agreements must be presented in writing within 3 calendar days of: 1) the release of this solicitation; or 2) the date the objector knows or should have known the basis for its objection.

Objections should be provided in letter format, clearly stating that it is an objection to this solicitation or to the conduct of the evaluation or award of an agreement, and providing a clear, detailed, and factual statement of the basis for objection.

Failure to comply with these directions is a basis for summary dismissal of the objection.
Mail objections to:

U. S. Department of Homeland Security
ATTN: Office of Procurement Operations
Margaret L. Graves
Team Lead/Contracting Officer
Science & Technology Acquisitions Division
7^{th} & D Streets, Room 3051
245 Murray Lane, S.W., Bldg. 410
Washington, DC 20528

3. Reporting

The following *minimum* deliverables will be required under traditional procurement contracts or other transactions agreements awarded to those offerors whose full proposals are selected for award.

Monthly Program Report

Brief narrative reports (not more than two pages) will be electronically submitted to the program manager within one week after the last day of each month (not more than two pages). These reports will describe: the previous calendar month's activity; technical progress achieved against goals; difficulties encountered; recovery plans (if needed); explicit plans for the next calendar month; and financial expenditures (including expenditures during the past calendar month period plus cumulative expenditures, and projected expenditures for the coming calendar month).

Final Technical Report

For a final report, each selected offeror will provide a technical report of work performed during the period of performance, delivered no later than the last day of the period of performance. The final report will be a cumulative, stand-alone document that describes the work of the entire test and evaluation period leading up to it.

It shall detail how the design prototype was refined or otherwise prepared for the test and evaluation program and, if applicable, why such refinements or preparations were undertaken. It must include any technical data gathered, such as measurements taken, models developed, simulation results, and formulations developed. The final report will include a summary of all performance goals versus performance achieved during the program, either measured or otherwise substantiated. The final report will discuss all variances from the performance goals versus performance achieved, including reasons or theories for variances.

If applicable, it will provide a discussion of how the offeror might meet any unmet performance goals under a future effort. This final report should also include "lessons learned" from the effort, and recommendations for future research, development, or testing that would lead to success in meeting the performance goals. The final report shall also provide a comprehensive and detailed account of all funds expended.

4. Project Meetings and Reviews

Program status reviews may also be held to provide a forum for reviews of the latest results from experiments and any other incremental progress towards the major demonstrations. These meetings will be held at various sites throughout the country. For costing purposes, offerors should assume that 40 percent of these meetings will be at or near DHS S&T, Washington D.C., and 60 percent at other contractor or government facilities. Interim

meetings are likely, but these will be accomplished via video telephone conferences, telephone conferences, or Web-based collaboration tools.

5. Additional Deliverables

Performers should define additional program-specific deliverables as appropriate for the proposed approach. The Government may describe additional deliverables at the time full proposals are requested.

VII. OTHER INFORMATION

1. Government Property, Government Furnished Equipment (GFE), and Facilities

The Government may provide government-furnished equipment (GFE), resources (GFR), information (GFI), or services (GFS) under the terms of each negotiated contract or agreement. GFE, GFR, GFI, or GFS requested by an offeror must be factored into the offeror's project cost. Each offeror must provide a very specific description of any equipment or hardware it needs to acquire to perform the work. This description should indicate whether or not each particular piece of equipment or hardware will be included as part of a deliverable item under the resulting award.

In addition, this description should identify the component, nomenclature, and configuration of the equipment or hardware that it is proposed to purchase for this effort. The Government wants to have the contractor purchase the equipment or hardware for deliverable items under its contract. It will evaluate case-by-case the purchase, on a direct reimbursement basis, of special test equipment or other equipment, not included in a deliverable item will be evaluated for allowability on a case-by-case basis. Maximum use of Government integration, test, and experiment facilities is encouraged in each of the offeror's proposals.

Government research facilities may be available, and should be considered as potential GFE. These facilities and resources are of high value, and some are in constant demand by multiple programs. The use of these facilities and resources will be negotiated as the program unfolds. Offerors should explain which of these facilities they recommend and why.

2. Security Classification

NO Classified White Papers or Full Proposals (or portions of proposals) will be accepted.

3. Information for White Paper and Full Proposal Respondents

This BAA is for planning purposes only. It will not be construed as an obligation on the part of the Government to acquire any products or services. No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of submission of responses to this BAA and the Government's use of such information. Respondents to this BAA may be

requested to provide additional information based on their submittals. Unnecessarily elaborate responses containing extensive marketing materials are not desired.

4. SAFETY Act

As part of the Homeland Security Act of 2002, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act"). The SAFETY Act puts limitations on the potential liability of firms that develop and provide qualified anti-terrorism technologies. DHS S&T, acting through its Office of SAFETY Act Implementation (OSAI), encourages the development and deployment of anti-terrorism technologies by making available the SAFETY Act's system of "risk management" and "liability management." Offerors submitting proposals in response to this BAA are encouraged to submit SAFETY Act applications for their existing technologies. They are invited to contact OSAI for more information, at 1-866-788-9318 or helpdesk@safetyact.gov. They also can visit OSAI's Web site at www.safetyact.gov.

EXHIBIT 3

"Proposal White Paper"

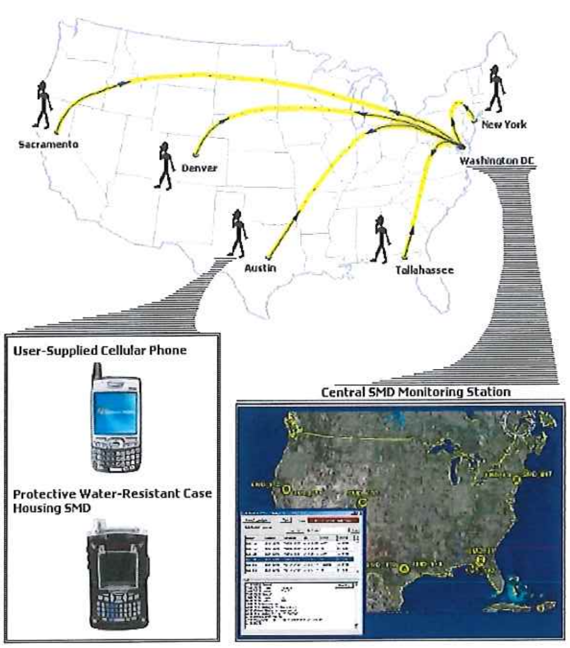
BROAD AGENCY ANNOUNCEMENT (BAA) 07-10

CELL-ALL Ubiquitous Biological and Chemical Sensing

Administrative and Technical Points of Contact:

Larry Golden, CEO
ATPG Technology, LLC
522 Peach Grove Place
Mauldin, SC 29662
864-288-5605 / 864-992-7104
lgolden5605@charter.net

Authorized Officer: Larry Golden

BAA Number: CELL-ALL BAA07-10 **Title:** CELL-SMD; Multi Sensor-Detection	**Offeror Name:** ATPG TECHNOLOGY, LLC **Date:** 11/28/2007
 	**Operational Capability:** 1. Ability to effectively sense/detect chemical agents, reliably and securely report position and detection readings. Provide software applications to easily manage large scale network. Design allows for straightforward integration with existing cell phones Ability to graphically depict and filter live data. 2. Goal: ability to detect chemical or biological agents 99%. Goal: network throughput 99%. 3. Prototype SMD(cell phone case) target cost is $50 in mass quantities (excluding sensor) Competition among sensor developers will drive final cost. 4. Durable, inexpensive device, does not degrade performance of host device Makes extensive use of existing technology and builds upon completed spiral of a similar device.
Proposed Technical Approach: 1. Provides Sensor Monitoring Device (SMD) in a protective cell phone case. Easy to distribute/integrate with cell phone Viewer/Management SW provides hierarchical levels for information flow 2. Incorporate selected sensors into existing SMD functional prototype Manufacture prototype cell phone cases to accommodate SMD and sensors Enhance/scale existing cell phone, web and desktop support applications 3. First spiral complete, yielded functional prototypes – SMD, web, desktop & cell phone applications 4. Established working relationships with Otter Box and ECBC 5. CELL-ALL technical approach & rational taken from, "Multi Sensor-Detection and Lock Disabling System", (Patent Pending; Pub., 10-18-07; App. #: 11/397,118:)	**Schedule, Cost, Deliverables, & Contact:** One year Period of Performance, $1,000,000 Prototype and manufacture cell phone cases with integrated SMD, chemical and biological sensors Enhance/scale viewer/management software to support large sensor network **Deliverables:** Prototyped cell phone case containing SMD and sensors Cell phone & desktop viewer/management SW System demonstration of: sensor detection, alert transmitted through hierarchy and control center messages to SMD **Corporate Information:** ATPG TECHNOLOGY, LLC Larry Golden, CEO 522 Peach Grove Place Mauldin, SC 29662 Phone: 864-288-5605 lgolden5605@charter.net

Executive Summary:

Two years ago, recognizing the danger that existed if a WMD was concealed, transported and deployed within our borders, ATPG embarked on the development of a multi-sensor, tracking and detection system. The first development spiral yielded a functional Sensor Monitoring Device (SMD) prototype and tiered communication applications to distribute, monitor and manage the multi-sensor SMD network information. The ubiquitous sensor network solution proposed in this white paper borrows heavily from the technology developed in spiral one. The tiered communication, viewer and management software applications were designed to be part of a large sensor network. For this application the software will be scaled and enhanced to accommodate the volume of traffic that would result from an extremely large sensor network. Our SMD was designed to provide as much flexibility as possible and communicates with a variety of sensors through an array of built-in standard interfaces (SPI, A/D, Serial, Bluetooth, I2C etc). This existing open architecture design affords us the opportunity to collaborate with the U.S. Army Edgewood Chemical and Biological Center (ECBC) to evaluate, test and acquire the most appropriate miniaturized chemical and biological sensors.

ATPG intends to utilize the hardware and software technology developed in spiral one as the basis for the ubiquitous sensor network. The form factor of the SMD will be re-engineered so that it can initially be housed in cell phone cases allowing straightforward integration with existing cell phones. The SMD, housed in the cell phone cases will use a Bluetooth channel to communicate with ATPG software hosted on the cell phone. This software will provide bi-directional communication between the SMD and cell phone. The cell phone software will additionally use email and SMS messaging services to communicate information to control centers. The software for managing the information from the sensor network will be architected in a way that provides a means to efficiently escalate information up the government hierarchy. The software will employ a large database back-end and where practical message routing rules will be implemented to allow for effective and efficient routing of sensor message traffic.

Utility to Department of Homeland Security:

ATPG's strategy of incorporating its existing SMD design into cell phone cases provides a means to quickly establish a massive sensor network nationwide. ATPG proposes modifying the SMD form factor so that it can be installed into the most common cell phone cases. When a person volunteers for the program they would receive a cell phone case along with an adapter cord that would connect to their existing phone charger; allowing the SMD and phone to charge simultaneously. A switch on the case will allow the volunteer to enable the device at their discretion. If a volunteer elects to participate in the program and their cell phone does not have an on board GPS, the SMD provided in the cell phone case will be equipped with one. The geographic position of the SMD/cell phone pair will be determined either by GPS, cell phone tower database and signal strength or by a Wi-Fi hotspot database. In the event current position cannot be determined, the device will use its last known good position fix for communications and the position will be flagged as such. Housing the SMD and sensors in a cell phone case provides a number of advantages. Since the SMD will draw all of its power from its own power source the only resources required from the cell phone will be for a dedicated Bluetooth channel and limited processing power to execute the cell phone software. Additionally the consumables

in the cell phone case (battery, sensors etc.) can easily be switched out, or the entire case can be easily replaced. ATPG will be working with the Otter Box Company to design a cell phone case capable of housing the SMD and its sensors, providing a protective, water resistant case while maintaining complete cell phone interactivity. This approach will allow ATPG to easily and incrementally make changes to the host platform as the technology of the SMD and its sensors are miniaturized.

Technical Approach:

The creation, implementation and management of a massive sensor network will require a design approach that delivers a system solution. Every tier of the system is important and the end product must be manageable, provide redundancy and implement an open architecture wherever possible. The ATPG solution proposed here focuses on these requirements and delivers a design that translates into a straightforward, deployable sensor network system that can be distributed en masse.

At the lowest level, the SMD is engineered to communicate with a variety of sensors through an array of standard interfaces (SPI, A/D, Serial, I2C etc). This open architecture allows for easily integrating additional sensors into the device and expanding the range of hazardous agents detectable by the SMD. The SMD will continually monitor/control the attached sensors and communicate with the cell phone via a dedicated Bluetooth channel. When the SMD is activated by the user, a small software application installed on the phone will monitors the Bluetooth channel for detection alerts and also forward commands received from control centers to the SMD. The SMD will periodically send its position information to the control center. The position the SMD will report to the control centers is determined using a layered approach. Initially the SMD will look to the on-board GPS (if provided) to determine position. If the cell phone is equipped with a GPS the application on the cell phone will retrieve the position from its own GPS. When a GPS position cannot be determined, the position of the SMD and its user will be calculated based on a cell phone tower database, provided by the FCC and signal strength. If this does not yield a result, the Wi-Fi hotspot database will be utilized to determine SMD and user position. If all these options fail, the last known position can be augmented with the on board accelerometers to estimate the current position which will be reported to the control centers and annotated as a last position and a possible position. All information received by the cell phone application from the SMD will be forwarded to the control centers either through email or SMS messages if email is not available. The information transmitted will be encoded in XML and encrypted prior to transmission. When a user needs to be notified of information from a control center, the cell phone software will use either a ring tone or vibration to call the user's attention to the display. This solution of integrating the SMD into the cell phone case and installing a small software application on the volunteer's cell phone provides a means to easily modify and upgrade the sensor network system as advancements are made to sensor and SMD technology with minimal impact to the user.

The web and desktop software that support the sensor network is designed to support an escalating reporting hierarchy. At each level rules can be established in the message routing software to facilitate the transfer of alert information. Rules can also be established to assist in determining the area affected by an alert. In the event a chemical or biological agent is detected

and reported, the software can automatically search for other sensors in a pre-defined area and command them to sample and report back. This information can then be used by first responders and local government to determine the impacted area and aid in creating a plan of action to cope with the event. The reporting hierarchy can be configured as needed but the current configuration sends notification to the local First Responder units, followed by City, County, State and Federal government. As the information works its way up the hierarchy rules at each level fire off to create events that notify necessary personnel at each level. The viewer/management software used at each level of the hierarchy is identical. How the system forwards and responds to data is configured in the message routing rules table. The desktop software uses Google Earth as a viewer and plots the position of the sensors and detections on the map. Filtering options are provided in the software to allow the screen to be decluttered. A hierarchical database of sensors reporting to the viewers at a given control center is maintained to allow simple manipulation of the sensor network. The software will allow the user to drill down into lower levels of the data by clicking on the images on the map or through the windows explorer like interface provided. The software will also allow commands and alerts to be sent to SMD enabled cell phones by clicking on the image or on its text representation. Each SMD representation on the map will display its unique identification number as its label and clicking on the icon will display the last set of data received by the control center. The sensor network data can also be made available to smart phones and PDAs running a variation of the viewer/management software. All data passed through this network will be encrypted and all database and user accounts will be protected by multiple layers of security to ensure the privacy of the volunteers and protect their location from foreign/unwanted access.

As an option all messages sent from the SMD to the control centers could receive notification of receipt; confirmation that the network is operating properly. This could be a built-in fail safe, which would allow the user to be notified first if detection occurred and the information could not be transmitted to a control center. In this scenario the user would be notified of the detection and could take action to leave the area and contact authorities through some other means.

Personnel and Performer Qualifications and Experience:

Larry Golden is the CEO of ATPG and will be the project manager for this program. Mr. Golden's invention and patent pending sensor monitoring device (Pub. 10-18-07; App. #: 11/397,118) will be used as the departure point for the development of the SMD. Mr. Golden's background is in industrial engineering and management. Larry's duties will include managing the schedule, budget and subcontractors providing the cell phone cases.

Harold Kimball is a software engineer with twenty years experience developing software applications, including embedded systems, operational flight programs, database applications, and web and desktop applications. Mr. Kimball will be the technical lead on this program as well as the lead software developer for the SMD applications. Over the past few years Mr. Kimball's focus has been on developing situational awareness applications, embedded device applications and aircraft simulation software. Mr. Kimball has a Bachelor's degree in Computer Science and is working on his Master's Degree in Artificial Life. Mr. Kimball recently had an

article published describing a scalable disaster relief and communications infrastructure system he is developing to aid first responders and disaster relief personnel in their efforts.

Doug Cumbie is an electrical engineer and software engineer with six years experience developing embedded systems, web applications, situational awareness software and aircraft simulation software. Mr. Cumbie will be the lead Engineer on this program as well as the primary developer for the web and desktop applications. Over the past few years Mr. Cumbie has focused on embedded device development, situational awareness applications and aircraft simulation software. Mr. Cumbie holds Bachelor's degrees in both Computer Engineering and Electrical Engineering.

The Otter Box Corporation will provide custom cell phone cases for housing the SMD developed by ATPG. The Otter Box Corporation has extensive experience manufacturing and distributing custom cases for cell phones, laptops and PDAs. Their manufacturing and distribution experience will play a key role in the ability to efficiently develop, manufacture and distribute a custom cell phone case enveloping the SMD and providing a water resistant and protective case.

U.S. Army Edgewood Chemical and Biological Center (ECBC) will play a vital role in assisting ATPG with evaluating, testing and selecting the most appropriate miniaturized chemical and biological sensors available. ATPG and ECBC have a collaborative agreement in place ensuring ATPG of their services in sensor analysis and selection.

Commercialization and Capabilities:

ATPG will work closely with Otter Box and ECBC to determine the physical characteristics and requirements needed to create a custom cell phone enclosure for the selected sensors and SMD. ATPG will leverage Otter Box's manufacturing and distribution experience to enable ATPG to produce and deliver large quantities of custom cell phone cases. As mentioned previously the case will be designed and developed so that consumables can easily be swapped out or the entire cell phone case can be replaced. This approach ATPG is pursuing is the most economical and efficient way to mass distribute a sensor network; providing low risk and minimal impact to volunteers of the program. Becoming part of this volunteer network would be a simple process and would only require end-users to; elect to become a volunteer, indicate which type of cell phone they currently use and upon receipt of the new cell phone case commence holstering the cell phone in the case wherever they go. As an option and to solicit interest in the program, volunteers could be provided software applications. These applications could potentially access tracking information of the volunteer's phone and the volunteer's family members' phones; or a moving map application could be provided to enable navigation through the cell phone. Mr. Kimball and Mr. Cumbie have many years experience developing and distributing code to demanding end users. Both individuals have experience providing Situational Awareness and OFP software to the Air Force Special Operations Command (AFSOC) for all fixed wing Special Operations Forces (SOF) aircraft. Additionally, Mr. Kimball worked for Manheim Auctions, an international organization with a large customer base and participated in the development and distribution of Manheim's software applications.

One method ATPG conceived for fielding the sensor network and implementing its widespread use would be to conduct a pilot program for the nearly 30 million government employees, border patrol personnel and government contractors. These individuals generally work in what would be considered high value target areas. Providing these employees with cell phone cases equipped with the SMD and its sensors would immediately give the sensor network nationwide coverage in many areas that would be likely targets of a terrorist attack. In addition to gaining nationwide coverage; if this pilot program extended to all government employees and its contractors around the world, the network would have the ability to monitor U.S. interests globally.

Costs, Works and Schedule:

The budgeted cost for this development is $1,000,000, with a projected period of performance of one year. ATPG will simultaneously commence four primary tasks upon contract award.

1) ATPG will work with ECBC to evaluate, test and select the most appropriate chemical and biological miniaturized sensors available (4 month effort, $17,137)).

2) ATPG will research and determine the three most commonly used phones capable of being part of this sensor network and work with Otter Box to design and manufacture cell phone cases to house the SMD and sensors (4 month effort, $45,000).

3) ATPG will enhance/scale the software applications to support the potentially large volume sensor network that will comprise the Cell-All ubiquitous system (7 month effort, $500,000).

4) ATPG will restructure and scale down the SMD so it can be accommodated in the cell phone case. After month 7, integration and testing of the Cell-All system will commence. The system will be documented (block diagrams, wiring diagrams, and theory of operation manual) and a demonstration date will be scheduled (12 month effort, $437,863).

Prototype cases housing the SMD and sensors, cell phones and viewer/management software executables will be delivered upon project completion.

Small Business Considerations:

This white paper is submitted from a minority owned small business.

EXHIBIT 4

DHS/S&T; Cell-All: Synkera Technologies

"Cell-All is managed and funded by HSARPA, the technologies and infrastructures are being developed by third party contractors who received funding from DHS for those purposes and who can then profit further from the sale of any resulting systems or services (U.S. Department of Homeland Security, 2011a,c). Currently, the primary contractors working on the project are Synkera Technologies, Qualcomm, NC4, and NASA's Ames Research Center…"

"Qualcomm's role has been to develop a smartphone app and the associated network software for processing data. Smartphone users can download the app from Google Play and, eventually, from Apple's iTunes store, so Cell-All will be operational on all phones using either Google's Android or Apple's iPhone operating systems. When the application is installed it will ask the user for permission to share sensor readings and location information over the network; then, whenever abnormal chemical levels are detected, the phone will send those data to a network gateway. According to Doug Hoffman, program manager at Qualcomm, the gateway will authenticate the sensor and phone to determine whether they are authorized to be on the network…"

"In order for the Cell-All public safety sensing and alerting system to be complete, four links must be forged and joined together: the sensor and computing hardware, the sensing application for mobile phones, a centralized server and network operations center, and the end consumer, whether individuals, emergency operations centers, first responders, government agencies, or private companies. Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded ''sleeve'' for phones—that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."

Torin Monahan, Jennifer T. Mokos (2013). Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks. *Department of Communication Studies*, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA. *Department of Human & Organizational Development*, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA

Geoforum 49 (2013) 279–288

Contents lists available at SciVerse ScienceDirect

Geoforum

journal homepage: www.elsevier.com/locate/geoforum

ELSEVIER

GEOFORUM

Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks

Torin Monahan [a,*], Jennifer T. Mokos [b]

[a] *Department of Communication Studies, The University of North Carolina at Chapel Hill, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA*
[b] *Department of Human & Organizational Development, Vanderbilt University, Peabody #90, 230 Appleton Place, Nashville, TN 37203-5721, USA*

ARTICLE INFO

Article history:
Available online 7 March 2013

Keywords:
Surveillance
Crowdsourcing
Mobile phones
Pollution
Outsourcing

ABSTRACT

Mobile systems for detecting environmental threats may radically restructure spatial imaginaries as people learn to see and engage with heretofore largely hidden dimensions of urban spaces. While the design of such technological systems is contingent and currently open to varied outcomes, powerful security and industry players are asserting their influence to set overriding protocols that will ensure widespread ambient data collection, especially for security and commercial applications. This paper critically explores the emergent power geographies of surveillance revealed by one such system: the Department of Homeland Security's Cell-All project. This project, which has been under development at the U.S. Department of Homeland Security (DHS) since 2007, equips mobile phones with chemical-agent detectors and links them to security networks so that threats to urban populations can be automatically detected and rapidly mitigated. In order to assess the politics of crowdsourced sensing systems, first we map the core characteristics of the Cell-All development model: creating a participatory system, building public–private partnerships, and outsourcing responsibility for privacy protections. Second, we describe some alternative designs for mobile, participatory environmental sensing and reflect on their potentials for correcting power inequalities or achieving environmental justice. Finally, we conclude by discussing the implications of these various systems and the conditions that could alter their outcomes.

1. Introduction

The securitization of urban spaces is a dynamic political process that mutates according to constructions of threat, need, and possibility. In some instances fear of terrorist attacks has motivated the hardening of potential targets, such as monuments or buildings, with video surveillance networks or concrete sacrificial facades intended to block would-be bombers (Boddy, 2007; Coaffee, 2004; Fussey et al., 2011). In other cases, unmanned aerial vehicles are deployed over cities and borders to watch for illegal or suspicious activities and direct authorities to investigate (Finn and Wright, 2012; Graham, 2010; Wall and Monahan, 2011; Weber, 2011). Other articulations come in the form of informatized passage points, such as building entrances, community guard stations, or airports, where biometric identifiers and identity documents can be checked to ascertain whether one should be granted access (Adey, 2006; Klauser, 2010; Lianos and Douglas, 2000; Magnet, 2011; Thrift and French, 2002). Such systems often act in overlapping and reinforcing ways, connecting with larger assemblages of regulation and control. As geographers and surveillance studies scholars have argued, the modalities of security systems are inflected by an anticipatory rationality that seeks to identify and control risks in advance (Coaffee et al., 2009; Graham and Wood, 2003; Haggerty and Ericson, 2006; Klauser et al., 2008; Lyon, 2003). Rather than being objective or deterministic, however, every step in the process—from risk construction to system implementation to altered practice—betrays a complex politics whereby resources are allocated, populations sorted, and institutions reconfigured.

An important dimension of the securitization process is the creation of compelling narratives to justify the surveillance systems under consideration. This mythical dimension relies on what Mike Crang and Stephen Graham (2007) have called "technological fantasies" that position emergent technological systems as necessary—and effective—responses to dire threats. Some of the genres at work are entertainment media and news reporting; police or government educational campaigns; and industry- and government-produced videos, presentations, and reports that typically describe scenarios of mass destruction, followed by proposed technological fixes to prevent or manage such crises (Altheide, 2006; Barnard-Wills, 2012; Graham, 2010). As has been argued elsewhere, technological fantasies are not simply instrumental narrative devices to achieve desired ends; in addition to this, they actively shape larger security cultures and afford them influence,

* Corresponding author.
E-mail addresses: torin.monahan@unc.edu (T. Monahan), jennifer.mokos@vanderbilt.edu (J.T. Mokos).

0016-7185/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.geoforum.2013.02.001

such that alternative motivations for personal or institutional action become filtered through a security lens (Monahan, 2010b).

The technological fantasy that is the backdrop for this paper is one where mobile phones are equipped with chemical-agent detectors and linked to security networks so that threats to urban populations can be automatically detected and rapidly dealt with. This project, which has been under development at the U.S. Department of Homeland Security (DHS) since 2007, operates under the name "Cell-All." It draws upon an existing ecology of related sensor networks woven throughout the built environment in many cities, such as Chicago's "Operation Virtual Shield," which includes smart CCTV cameras and hidden chemical and biological agent sensors (Bulkeley, 2009; Murakami Wood, 2009a). The name Cell-All references the ubiquity of mobile phones and perhaps unintentionally signals the data exchange made possible by the public–private partnerships that are at the heart of this enterprise. The DHS Cell-All project is also designed to exploit mobile-phone saturation to enroll everyday users as passive data collectors whose devices communicate silently to the DHS system and its private industry partners. As with U.S. border-control and military efforts to enlist citizens as participants in crowdsourced surveillance (Koskela, 2010; Murakami Wood, 2009b), the success of Cell-All depends upon a mass of participating individuals scanning public spaces.

The ideological underpinning for the Cell-All project is one of neoliberal public–private partnerships, by which industry profits from privileged government contracts and access to data without accepting many financial or symbolic risks. A core component of this arrangement, as will be shown, is in the persuasion of everyday mobile phone users to act as data collectors and distributors. In this sense, to achieve initial success a certain type of participatory surveillance must be cultivated through discursive appeals to individuals—whether patriotic duty to avert mass-casualty disasters, personal interest to save oneself or one's loved ones from carbon monoxide poisoning, or individual desire to be a part of an innovative technological research project. Regardless of the nature of the appeal, the intended outcome is for the responsibilization of individuals to undertake what Mark Andrejevic has referred to as the "work of being watched," an eager involvement in data collection and restricted forms of interactivity that may give one pleasure while simultaneously serving the interests of institutions (Andrejevic, 2002, 2007).

While the Cell-All project may rely upon a technological fantasy, it is certainly not fictional. Prototypes have already been developed, major telecommunications companies have become partners, and mass-marketing strategies are being fine-tuned. Drawing upon insights from the field of science and technology studies, one could say that the "black box" of this technology is rapidly closing and its politics are solidifying; as a result, alternative, perhaps more democratic and empowering possibilities are being foreclosed (Akrich, 1992; Winner, 1986; Woodhouse et al., 2002). Once mobile phone manufacturers routinely include chemical and other sensors in their devices, users can be compelled or coerced to communicate environmental data as such sharing becomes normalized in technical protocol. There is precedent in place to require geolocational data sharing as an "always on" feature of mobile phones for purposes of public safety under the E911 initiative in the U.S. and similar requirements in other countries (Curry et al., 2004), so one can easily envision similar policies mandating the constant relay of environmental readings. This predictable development makes sense in part because of the widespread normalization of surveillance through commonplace media and organizational encounters. As David Murakami Wood and William Webster explain: "Interactions become structured around surveillance relationships and the new forms of social negotiation that emerge are no longer about what information one chooses to give but how that information is to be given (or taken)" (Murakami Wood and Webster, 2011: 157).

In keeping with the goals of this special issue, this paper will critically explore the emergent power geographies of surveillance revealed by DHS's Cell-All project. Environmental sensing with mobile devices represents, on one hand, the possibility for crafting new spatial imaginaries and modes of public engagement that bring about collective empowerment. On the other hand, technological systems must be situated within their current political and ideological contexts, which in the case of Cell-All signifies a tightly constrained trajectory for technology development that promises coerced participation and asymmetrical relationships of visibility. First, we will provide an overview of our methods and sources. Second, we will draw upon DHS documents and presentations to analyze the Cell-All project, paying particular attention to the core characteristics of its development model: creating a participatory system, building public–private partnerships, and outsourcing responsibility for privacy protections. Third, we will describe some alternative designs for mobile, participatory environmental sensing and reflect on their potentials for correcting power inequalities or achieving environmental justice. Finally, we will conclude by discussing the implications of these various systems and the conditions that could alter their outcomes.

2. Methods and sources

The primary case study analyzed here—that of the Cell-All system—is based on a review of official and public documents, including press releases, media reports, DHS documents and training materials, and commercial partner marketing products and websites. We conducted a LexisNexis news search to identify news, media, and publicly available materials referencing Cell-All. All articles returned by the search were examined for relevance, and those not directly discussing the Cell-All program were discarded, with 31 documents remaining. These relevant documents were read and coded to identify initial thematic concepts in accordance with grounded theory approaches to data analysis (Charmaz, 2006).

In response to initial thematic coding, additional targeted data collection was focused on DHS and commercial partner documents and websites in order to identify the current development status, the operation and functionality of the system, and marketing strategies. This secondary investigation included a thorough search for pertinent documents on DHS's website, as well as searches on commercial partner websites, to locate original agency and company texts. A 2-hour video webcast of the DHS's live demonstration and training of the Cell-All project held at the Los Angeles Fire Department's Frank Hotchkin Memorial Training Center on September 28, 2011 (U.S. Department of Homeland Security, 2011a) was also transcribed and coded. Analysis of primary DHS and commercial partner documents yielded key information on the design of the Cell-All system, from the environmental sensors to the broader support and data communication infrastructures developed to store, analyze, and send alerts.

Many of the media and news articles identified were printed in security trade publications, such as Aviation Today's *Air Safety Week* and the *Terror Response Technology Report* (*TR2*), and they were often published in response to press releases from DHS or other Cell-All partners, such as NASA's Ames Research Center. This dynamic tended to produce clusters of articles with similar headlines and content that often closely reproduced the phrasing and content of the agency press releases. Similarly, the few articles that did appear in the mainstream media seemed to echo statements made in press releases with little or no analysis. This relationship between press releases and media reports suggests that there

may be a disproportionate ability afforded to DHS and commercial entities to shape public understanding and uptake of these technological systems.

3. Exploring the DHS Cell-All project

3.1. Project background and development

Cell-All is a program managed by DHS to develop software and hardware that enables smartphones to function as handheld, pervasive environmental sensors. In the initial research and development phase, engineers miniaturized sensors to detect abnormal levels of potentially dangerous chemicals in the surrounding environment. When dangerous levels are detected, an application on the cell phone should automatically send sensor and location data over the network to a centralized server, which will then contact appropriate agencies and first responders. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones.

The Homeland Security Advanced Research Projects Agency (HSARPA) of the DHS Science and Technology (S&T) Directorate refers to the sensors as "a new class of chemical detectors" that are smaller, less expensive, and *in situ* compared to the fairly large, static, and relatively expensive sensors used at existing monitoring stations (U.S. Department of Homeland Security, 2011a). By drawing upon mobile phone saturation, the Cell-All program aims to establish a flexible and dynamic sensor system, with citizens functioning as roving information nodes. As Stephen Dennis, the technical director of HSARPA, states, "Generally people have their smartphone with them. It's representing [through sensor readings] the space that they reside in" (Dennis, 2011).

For the program's initial phase in 2007, DHS released a call for proposals inviting the private sector to develop a proof of concept for the "Cell-All Ubiquitous Biological and Chemical Sensing" project (U.S. Department of Homeland Security, 2007). The goals at this point were to design a range of chemical sensors and refine the GPS functionality of phones to achieve accurate transmission of location data. According to DHS, the first year and a half focused on the question "Could we miniaturize chemical sensors and make them actually fit a cell phone profile?" (Dennis, 2011). Thus, researchers focused on understanding the needs of the equipment, in terms of power and physical profiles, and determining whether the sensors could work within the "ecosystem of the phone." HSARPA conducted a national search for ideas that was intended to leverage existing technological expertise in the public and private sectors, which led to the creation of six workable first-generation prototypes, including a "form factor phone" developed by Qualcomm and a chemical nanosensor device developed by NASA (U.S. Department of Homeland Security, 2011a).

The second phase of Cell-All began in 2010 with the goals of creating dozens of competing viable devices and refining the network capabilities of the system (U.S. Department of Homeland Security, 2011a). At this stage, DHS also sought to standardize the data-reporting protocols so that data from different devices could be received and processed by a centralized network operations center. Research contracts were awarded by DHS through HSARPA and the Small Business Innovation Research Portfolio, with some of the primary recipients being Qualcomm, Synkera Technologies, and NASA (U.S. Department of Homeland Security, 2011b). In addition, DHS S&T secured Cooperative Research and Development Agreements with four primary cell phone manufacturers—Qualcomm, LG, Apple, and Samsung—with the objective of accelerating the "commercialization of technology developed for government purposes" (U.S. Department of Homeland Security, 2010).

During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones (U.S. Department of Homeland Security, 2011a). This use of third-party accessory products is intended to speed up the technology's commercial availability so that people can begin using the Cell-All applications with their current phones before integrated sensors are fully operational and readily available. At a September 2011 live test and demonstration of second-generation prototypes at the Los Angeles Fire Department's Frank Hotchkin Memorial Training Center, Synkera's prototype was already on the market and NASA's sensor was awaiting clearance for public release. DHS presentations at this event conveyed that next generation, sensor-embedded phones would roll out gradually over the next few years and, as with cameras in phones, would soon become standard (U.S. Department of Homeland Security, 2011a).

3.2. Cultivating participation through a personal alerting system

A 2011 report by Fox News begins with the following scenario: "A silent killer threatens a family with a baby in a hotel room. Fortunately, their smartphone wises up, senses the threat and notifies the authorities—and the local fire department charges in to the rescue, saving the day" (Barrie, 2011). The silent killer in this story is that of carbon monoxide, which causes thousands of poisonings and hundreds of deaths each year (King and Bailey, 2007), and the smartphone is equipped with gas sensors and linked directly to DHS's Cell-All system, allowing for automatic communication with first responders. The fictional story continues by escalating the life-saving potential of the systems to mass casualty terrorist attacks:

> Ultimately, Cell-All could be American's secret weapon against public threats at football stadiums or sarin gas-style attacks like the one that killed 13 people in Tokyo's subway system in 1995. Experts are always working hard to find ways to reduce the risk to Americans at large events that could be attractive targets to terrorists. (Barrie, 2011)

As with other surveillance systems deployed under the rubric of counterterrorism, the accompanying narrative implies technological infallibility and nurtures public support through a process of simplification that strips away politics and social difference (Monahan, 2010b). What is especially interesting about this media thread, though, is that it emphasizes personal, commonplace threats (carbon monoxide poisoning of families) over large-scale terrorist attacks. This may indicate a larger shift in security discourses, but it also suggests an intentional crafting of message, on the part of DHS and its partners, to encourage participation of and support by the growing population of smartphone users in the U.S.

Therefore, during the second phase of development outlined above, DHS shifted its marketing strategy to stress the personal protection aspect of the project as an approach intended to persuade consumers to buy the associated products (U.S. Department of Homeland Security, 2011a). So, whereas in 2010 media articles and a DHS press release focused on the homeland security potential of the sensors to detect biological and chemical terrorist agents, for example by calling it a "handheld weapon of mass destruction detector" (U.S. Department of Homeland Security, 2010), in 2011 the technology was instead described as a "personal environmental threat detector system" (U.S. Department of Homeland Security, 2011c: 37) and an "environmental surveillance system" (U.S. Department of Homeland Security, 2011b: 2). By the time of the 2011 Cell-All product demonstration, presenters

concentrated almost exclusively on threats posed by commonplace gas or chemical exposure, such as carbon monoxide in the home or toluene in nail salons. Furthermore, while a range of sensors are available to detect chemicals, such as chlorine, carbon monoxide sensors were the ones first linked to the Cell-All platform and made available for purchase (Li, 2011).

Unlike most state-sponsored security programs, which are implemented without full public knowledge or direct approval, the public–private partnership model adopted by Cell-All requires public buy-in, at least initially. This necessitates the adoption of a market lens to evaluate the need for and potential success of this public safety program. As DHS's Stephen Dennis explained, "We didn't just do the science work here; we actually did look at the market" (Dennis, 2011). With Qualcomm's help, DHS assessed commercial viability through market research, asking what conditions would need to be met for the public to both accept and pay for the system. Based on this market research, DHS concluded:

> What we learned is that the personal protection application will sell the device. People will actually turn in their [current] phone, get a new phone, if it provides them with a magnitude of personal protection, especially for families, people with aging parents, people with young children. (Dennis, 2011)

In order to convince people that the system would assist with personal protection, DHS settled on carbon monoxide poisoning as a much more likely and avoidable threat than terrorism. Mainstream media outlets like Fox News could provide sensationalistic sales-pitch stories about the "silent killer" of families with babies, while DHS could craft an argument drawing upon sober statistics and the expertise of first responders:

> When we asked our nation's first responders to name the deadliest gas for us, in terms of what the American population faces as a threat, carbon monoxide was it... it actually establishes a basis for commercial manifestation of what we've done here. (Dennis, 2011)

Thus, by the time of DHS's live demonstration of their system in 2011, the entire framing had shifted to "infiltrations" of carbon monoxide as an invisible and unpredictable danger to Americans:

> Today's test is going to focus on a common poisonous gas that is responsible for more than 2,000 deaths in the United States every year. As a matter of fact, just yesterday there were 43 people injured in an incident in Washington D.C. where carbon monoxide gas infiltrated into a building. (Verrico, 2011)

The marketing efforts that follow these threat constructions focus almost exclusively on the individual, positioning the product as a personal alerting system.

As a personal sensing and alerting system, Cell-All promises to protect a diverse and inclusive range of individuals, from "a grandmother taking a siesta [to] a teenager hiking through the woods..." (U.S. Department of Homeland Security, 2010). When set to personal safety mode, an auditory alarm will sound directly on the phone when the sensor detects an abnormal chemical level, and the app can also be configured to send a text message to specific emergency contacts designated by the user. While the sensing data ostensibly remain within the sphere of users and their designated contacts, in order to take advantage of these data for other purposes, such as ensuring public safety, the program includes plans for automatically reporting personal alerts to an independent monitoring service (U.S. Department of Homeland Security, 2011a). By expanding the data network in this way, DHS hopes to harness the collective potential of mobile phones as public environmental sensing devices for "crowdsourcing human safety" (U.S. Department of Homeland Security, 2010).

As a starting point, users will be given the choice of opting-in to wider sharing of their sensing data:

> We're asking the public if they would like to opt-in to a network, an anonymous network, an anonymous report, of what is it that their phone has seen to an operations center that can then understand what it is that that sensor and the collection of sensors around them actually means in terms of response. (Dennis, 2011)

One can note in this articulation the incipient unfolding of an argument for access to—and control of—data by organizations that can "understand" what an alert "actually means." Beyond the personal alert functionality, the larger goals are to aggregate data from multiple cell phones located within crowded public areas, such as sports arenas, subway stations, or office buildings. Then in addition to sending an individual alert, each phone on the network could send abnormalities detected by the sensors directly to a centralized network operations center (NOC). The idea is that the NOC will be equipped to analyze the reports within the context of each other (as well as other available data) and the aggregation of sensors in crowded public places will minimize false positives. One phone reporting an abnormal chemical level could be an error; a hundred phones reporting the same levels would be more likely to indicate a situation in need of intervention. When the NOC identifies that a threat is likely, it could then contact local agencies and first responders.

In order for Cell-All to succeed as it moves along a path from personal protection to centralized data collection, it must both compel and automate participation in data-sharing schemes. DHS rationalizes this as placing trust in objective technological systems instead of supposedly unreliable and error-prone individuals:

> Currently, if a person suspects that something is amiss, he *might* dial 9-1-1, though behavioral science tells us that it's easier to do nothing. If he does do something, it may be at a risk to his own life...the caller may be frantic and difficult to understand, diminishing the quality of information...An even worse scenario: the person may not even be aware of the danger, like the South Carolina woman who last year drove into a colorless, odorless, and poisonous ammonia cloud. (U.S. Department of Homeland Security, 2010)

In this example, it is not obvious how a cell-phone sensor would have helped, and according to other sources the woman, who died, left her vehicle because she was aware of the gas (Associated Press, 2009). Still, the example hints at scenarios where an automated Cell-All system might save lives, such as if multiple sensor readings prompted a rapid evacuation and quarantine of contaminated areas. Automated data sharing, a fully functional infrastructure, and tight coordination with first responders would be necessary components for this to be effective.

In the marketing of Cell-All, personal protection serves as the initial hook, allowing for data sharing to be expanded gradually. First this will take the form of opting-in to sharing data with a network operations center, with assurances that personal identifiers will be scrubbed from the data. Next, if precedent holds, wider data sharing will occur and participation will become compulsory. A neoliberal ideological context shapes the Cell-All project as a whole, as we will discuss further in the next section, but it also motivates government agencies to formulate problems in such a way that market-based solutions become logical responses to them.[1] Therefore, rather than tackle the health dangers posed by

[1] The neoliberal context signifies, in part, a market rationality of privatization of public goods and institutions, deregulation of industry, and responsibilization of individuals for the provision of human security and social reproduction (Monahan, 2010a, 2010b).

cumulative exposure to contaminants or impose tighter regulations upon chemical and other polluting industries, DHS focuses on individual responsibility for mitigating threats as a gateway to supposed wider public protection from catastrophic events. Just as individuals are being charged with maintaining the integrity of their digital identities online (Whitson and Haggerty, 2008), Cell-All hints at new articulations of responsibility where individuals will be enlisted symbolically as data collectors of environmental threats, fulfilling their biochemical duty to keep themselves and their families uncontaminated.

Enrolling members of the public could be seen as an entrepreneurial move on the part of DHS to exploit existing public resources, in the form of people with smartphones, to meet its narrowly defined public-safety objectives; as a Qualcomm representative argued: "Let's take advantage of the 300 million cell phones that are out there today. They're always with us" (Hoffman, 2011). Widespread participation is needed, with members of the public serving as passive data-collection nodes, but the program's goals do not include promoting environmental expertise among everyday users. The model for achieving such protection depends on centralized data collection so that experts and authorities can act to minimize or respond to threats. Although public protection may never actually be achieved by this system, it nonetheless advances public–private partnerships that further normalize the collection of sensitive, personal data for purposes of profit and control.

3.3. Forging public–private partnerships

The Cell-All program is funded and managed by HSARPA, whose mission is to facilitate the rapid development *and* deployment of new security technologies, mainly through partnerships and contracts with the private sector (U.S. Department of Homeland Security, 2011a). As DHS representatives explain it:

> The most important component of all is delivering the technology into the hands of those who need it so that we're not one of those government R&D labs that's happy to throw something over the wall or end it with a paper. We're actually trying to take this technology all the way to the end. (Dennis, 2011)

HSARPA accelerates this process through direct commercial partnerships, where it funds researchers from both the public and the private sector to develop products that can then be brought to market, even if the only buyers are government agencies.

The resulting neoliberal arrangements mirror those in other industries—such as pharmaceutical research and development, where in the U.S. the vast majority of research is paid for by public funds and conducted in university labs, after which time pharmaceutical companies acquire those research findings to develop profitable drugs without distributing revenue back to the public sector (Angell, 2004; Fisher, 2009). More than simply being pro-business, such arrangements seek to privatize government functions through partnerships and reconstruct the public good as that which benefits industry. Public subsidization of private companies, whether in the domains of homeland security or pharmaceuticals, is rationalized through discourses of efficiency. In the example of Cell-All, DHS justifies such partnerships by saying:

> We believe that technology transfer directly to the commercial [sector] is an efficient way to go. We know that there are a number of commercial opportunities that have been provided to our sensor manufacturers and to the folks who are involved in this program, so we're looking forward to taking advantage of those [opportunities] directly. (Dennis, 2011)

Therefore, although Cell-All is managed and funded by HSARPA, the technologies and infrastructures are being developed by third party contractors who received funding from DHS for those purposes and who can then profit further from the sale of any resulting systems or services (U.S. Department of Homeland Security, 2011a,c). Currently, the primary contractors working on the project are Synkera Technologies, Qualcomm, NC4, and NASA's Ames Research Center, which is the only public agency receiving a contract.

Each of the organizational entities involved in the project are working on separate system components that will be integrated as the project progresses. The exception is the NASA research center, which appears to be on a parallel development track to the industry partner Synkera, although it is not clear how much intellectual property is being transferred from NASA to Synkera or the other companies. In order for the Cell-All public safety sensing and alerting system to be complete, four links must be forged and joined together: the sensor and computing hardware, the sensing application for mobile phones, a centralized server and network operations center, and the end consumer, whether individuals, emergency operations centers, first responders, government agencies, or private companies. Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded "sleeve" for phones—that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011).

Qualcomm's role has been to develop a smartphone app and the associated network software for processing data. Smartphone users can download the app from Google Play and, eventually, from Apple's iTunes store, so Cell-All will be operational on all phones using either Google's Android or Apple's iPhone operating systems. When the application is installed it will ask the user for permission to share sensor readings and location information over the network; then, whenever abnormal chemical levels are detected, the phone will send those data to a network gateway. According to Doug Hoffman, program manager at Qualcomm, the gateway will authenticate the sensor and phone to determine whether they are authorized to be on the network, scrub personal information from the data, assign a temporary identification number to the phone, and then send data to the network operations center (NOC) (Hoffman, 2011).

The NOC acts as a data-clustering algorithm that combines and analyzes data from multiple phones in terms of geographical location, time, and chemical level in order to determine whether there is an abnormal public safety event. The NOC servers also have the ability to communicate directly with phones to change the frequency with which the phone is reporting data. For example, if there is a major risk-event involving many cell phones, the NOC can request less frequent reporting so that the network is not overloaded.

If the NOC algorithms determine that there is a potentially dangerous situation, an alert is transmitted to a "risk center" run by the California-based security company NC4. Established in 2001 after the attacks of 9/11, NC4 specializes in "situational readiness," which it aspires to obtain by bridging "the communication gap in a post-9/11 environment between the public sector and the private sector" (Needs, 2011). NC4's customers include both private and public sector organizations oriented toward security, risk management, and emergency response. The company operates two "risk centers," one on each U.S. coast, where analysts receive and vet data from NOCs and other sources before communicating threats to others or assisting with responses. Essentially, NC4 risk centers function as private-sector "fusion centers," much like DHS data fusion centers that are intended to identify threats in advance, assist

law-enforcement investigations, and coordinate responses (Monahan and Palmer, 2009).

According to Chris Needs, product and content manager at NC4, the risk centers perform a "human-in-the-loop" function of looking at raw data from the sensors, comparing them with data from other sources, and translating them into alerts that can be sent, for a fee, to end users, whether first responders, government agencies, individual consumers, or private-sector commercial entities.[2] For example, during the Cell-All live demonstration in 2011, alerts were sent to the Los Angeles emergency operations center, which could have then dispatched first responders or managed the threat were it real. The service provided by NC4's risk centers is marketed as generating "value-added" alerts that can include maps of locations with spikes in sensor readings, "so if you're not familiar with the area you can see how far is this incident from my sensitive assets" (Needs, 2011).

There is certainly a great deal of coordination required by DHS to bring the program components together for Cell-All to even approach operational status. From the start, though, the program has fostered public–private partnerships under the assumption that government agencies are too slow or lack the expertise to develop such a system on their own. This position is neatly articulated by HSARPA:

> The acceleration of integrated environmental sensing and the utilization of mobile computing platforms for homeland security establishes a leading edge capability instead of a traditional trailing edge capability that government sometimes has, taking advantage of the latest in new chemical sensor innovation. Delivering these capabilities to the extended homeland security enterprise as a commercial capability makes government technology transfer easier and far more efficient than trying to nurse it along inside of government, so I'm very excited that we have commercial opportunities to take advantage of the technology that's been created here. (Dennis, 2011)

NC4's CEO and president Jim Montagnino puts it a bit more bluntly, actually implying that government bureaucracies invite security threats: "Bureaucratic red tape impedes critical information sharing across organizational boundaries, which leaves the door open to national security threats" (Montagnino, 2012).

Framed in this way, the expedient solution is neither to concentrate on problems that government is equipped to solve, such as passing and enforcing environmental regulations, nor is it to streamline government agencies, although that option certainly exists as an imperative within neoliberal cultures. Rather, the task is seen as finding ways to entice industry to "partner" with government agencies, mainly by ensuring profitability for private companies (Monahan, 2010b). This orientation is evinced by Cell-All's early-stage market research, paid for by HSARPA and administered by Qualcomm. After finding a viable market, industry partners were further persuaded by government contracts to develop systems and services and by the high probability of sustained profits from a range of customers after product development. Clearly, having privileged access to consumer data, even in de-identified, aggregate form, would be of great interest to partnering companies.

3.4. Outsourcing privacy protections

During the research and development phase of projects like Cell-All, privacy risks are the responsibility of DHS's S&T Directorate, which conducts privacy impact assessments (PIAs) for laboratory- and field-testing. However, once S&T raises a technology to operational status, the responsibility for evaluating emerging privacy risks typically falls upon the privacy offices of the respective entities involved, such as Immigration and Customs Enforcement, the Transportation Security Administration, the Coast Guard, or others (U.S. Department of Homeland Security, 2011c). This separation between research and operational responsibilities for privacy protection may have particular implications for Cell-All because the final deployment of the technology will also have a commercial component. When government entities constitute the end-user community, the DHS Privacy Officer may require that privacy impact assessments be incorporated into the implementation process (Clarke, 2009); however, the private companies that will be managing core components of Cell-All are under no such obligations.

While one might expect that the early-stage PIA conducted by DHS would nonetheless anticipate real-world operational deployments of Cell-All, this is not the case. Instead the focus is on ensuring privacy protections for the development and pilot-testing phases (U.S. Department of Homeland Security, 2011b). To accomplish this, DHS adopted what is akin to institutional review board (IRB) review for human subjects research, including obtaining informed consent from participants. Thus, for a 2011 personal safety demonstration of Cell-All at the Los Angeles Fire Department test facilities, first responders participating in the demonstration consented to the transfer of geolocational data over the network but not personally identifiable information, such as mobile phone numbers (U.S. Department of Homeland Security, 2011a). As is standard with informed consent for research, "users participating in the test [were told that they] may turn off their cell phone and stop participating in this test at any time" (U.S. Department of Homeland Security, 2011c: 38). After testing is complete, however, the system "will be transitioned to the private sector and marketed by commercial vendors" (U.S. Department of Homeland Security, 2011c: 39), such that responsibility for privacy protections will be handed-off to those companies.

The model of outsourcing privacy protections to private companies engenders some interesting discursive moves on the part of DHS representatives, who say things like: "While Cell All was designed with privacy protections in mind, the end user community must continue to consider privacy when deploying the system for operational use" (U.S. Department of Homeland Security, 2011b: 7). After deployment, those managing the system will determine whether they want to collect cell phone numbers, users' locations and movement, or all chemical readings, rather than only ones deemed "significant." This position is made clear by a DHS privacy impact assessment that states:

> Decisions regarding the capture and transmission of additional information (e.g., phone numbers, names of cell phone owner) will also be decided by the end user community, with input from the first responder community, and public health organizations, among others. (U.S. Department of Homeland Security, 2011b: 6)

DHS dismisses any future privacy concerns by implying that individual users will always be able to opt-out of the system if they feel uncomfortable: "Privacy is as important as technology... After all, for Cell-All to succeed, people must be comfortable enough to turn it on in the first place" (U.S. Department of Homeland Security, 2010). For DHS, operational risks are narrowly defined in terms of market failure, not potential problematic uses of personal data, lack of transparency about data being collected and shared, or the coercive effect of technological protocols that may resist easy rejection.

As has been demonstrated with other dimensions of surveillance societies, private companies have an interest in amassing

[2] The NC4 analysts continually monitor multiple government and media information streams, including social media.

as much personal data as possible in order to profit, whether by selling convenient products and services to users, providing data for a fee to government agencies, or minimizing risk more generally (Andrejevic, 2007; Lyon, 2001; O'Harrow, 2005). Without specific prohibitions against the collection and use of personal data, projects like Cell-All possess a strong valence toward applications that exceed the original scope of the project. The data produced from the system can also be funneled back to government agencies, just like DHS fusion centers pay to tap the repositories of private data aggregators to assist with investigations, even if such data would be illegal for fusion centers to collect on their own (Monahan and Palmer, 2009). In such situations, the systems can effectively evade public accountability because private companies, who maintain the databases, are shielded from open-records requests.

Privacy threats extend beyond the coercive collection and storage of personal information. Control over who has access to such information is also tenuous, as can be seen, for example, with the numerous cases of hundreds of thousands of electronic records of personal information being hacked, lost, or stolen—from private companies and government agencies alike (Gilliom and Monahan, 2013). Furthermore, even if accessed in aggregate form, data mining and big data analytics can produce startlingly accurate profiles, which could be used to further sort, discriminate against, or commercially target users (Andrejevic, 2011). Data analytics of commercial systems have also revealed the ease with which individual users can be reidentified, even when anonymity has been ensured (Gilliom and Monahan, 2013). Thus, Cell-All and similar systems further the process by which individuals become sensing nodes themselves, communicating valuable data to private companies, government authorities, and peers.

With Cell-All, there is also strong potential for mission creep because of organizational arrangements that make robust privacy protection voluntary and mobile technologies that afford the collection of highly granular data. As Katie Shilton has observed, "At the extreme, mobile phones could become the most widespread embedded surveillance tools in history" (Shilton, 2009: 48). When coupled with environmental sensors, the capacity of mobile phones to identify individuals and track their movements could lead to many kinds of social control and discrimination well beyond the disclosure of personal information. For instance, insurance companies could use such data to cancel an individual's medical coverage or increase premiums because one is routinely exposed to high levels of air pollution because of where he or she lives, works, or commutes. This is not that far fetched as there are existing corollaries with companies charging higher rates for property insurance when people live in high-crime areas, or with companies offering "lifestyle discounts" for people who can prove that they exercise regularly and eat healthy foods (Gilliom and Monahan, 2013). Other scenarios could include companies using sensor data from individuals' phones to make decisions about whom to hire or which employees to discipline; just like organizations currently can demand drug testing, sensor-embedded phones could reveal who is exposed to marijuana or tobacco smoke and therefore who might be deemed to be a risk to the company. The same might hold true for landlords requesting sensor data as a condition for considering tenants' applications, just as many landlords presently require credit checks when considering applications (Neighborhood Link, 2010). This list of examples could easily be expanded, but the point is that based on precedent such systems will lend themselves to coerced participation and sorting of populations based on perceived risk levels, so these outcomes should be anticipated in advance of system deployment.

4. Toward empowering participatory sensing

Cell-All serves as an influential case study, particularly because the program shapes technological designs and organizational models that will guide future endeavors in the area of mobile environmental sensing. It advances a dominant paradigm of surveillance predicated upon asymmetrical relations of visibility and control, on one hand, and industry profits, on the other. Additionally, as a case study, Cell-All is emblematic of wider trends in the development of restrictive spatial protocols for locational tracking and sensing. As socially constructed systems, though, such spatial and technological protocols need not be so restrictive, extractive, or controlling. A variety of alternative, more open and participatory designs are circulating, even as DHS and its industry partners are moving toward technological closure on mobile sensing systems.

Several scholars have been actively involved in theorizing such alternative surveillance trajectories, often in conversation with artists, engineers, and activists. For instance, David Murakami Wood has described the possibility of shared surveillance protocols that might build upon the inclusive ideals of universal design and open source movements to enrich people's lives and produce relationships of sociality (Murakami Wood, 2007). Katie Shilton, working through a number of persuasive case studies, refers to participatory sensing as an activity that "is meant to enable (and encourage) anyone to gather and investigate previously invisible data. It tries to avoid surveillance or coercive sensing by emphasizing individuals' participation in the sensing process" (Shilton, 2009: 50). Dana Cuff, Mark Hansen, Jerry Kang argue for embedded-network-sensing applications that advance social empowerment through the creation of a "data commons" that functions as "a data repository generated through decentralized collection, shared freely, and amenable to distributed sense-making not only for the pursuit of science but also advocacy, art, play, and politics" (Cuff et al., 2008: 29).

Many of the projects being developed by UCLA's Center for Embedded Networked Sensing (CENS) attempt to catalyze empowering participatory sensing. For example, the Personal Environmental Impact Report (PEIR) project encourages individuals to use their mobile phones as self-surveillance devices to track their daily exposure to air pollution and calculate their own carbon footprints (Shilton, 2009, 2012). By reading locational data against air-quality alerts and maps, the system determines the amount of pollution one is exposed to over a given time period. Also, by drawing upon the GPS and accelerometer sensors in most mobile phones, PEIR can surmise what mode of transportation one uses for commutes and estimate one's carbon footprint based on those data. The overall aim is clearly one of cultivating public awareness of pollution problems and motivating individuals to change their own behavior to minimize both exposure and contributions to air pollution. Beyond this, CENS seeks to push participatory sensing toward democratic and environmental justice outcomes, encouraging mobile phone users to document egregious pollution conditions, share those data with others, and mobilize findings—in consultation with scientific experts—to influence policymakers (Center for Embedded Networked Sensing, 2008). Although the vision does problematically imply that one could uncover indisputable truths that would necessarily lead to progressive policy changes, the power of this model of participatory sensing is in its semi-open protocol that foments new spatial imaginaries about pollution in urban environments and invites participants to use data for their own ends, whether for changing individual behaviors or organizing for social change.

Another provocative example is the Safecast system, which originated as a collective of individuals using mobile phones and

Geiger counters to map radiation levels in Japan during the nuclear crises precipitated by an earthquake and tsunami in 2011. During this period, many people purchased radiation detectors and shared "readings" through websites and social media as a mechanism by which to achieve collective knowledge about dangers when official information was seen as being insufficient or untrustworthy (Safecast, 2012). The Safecast network, which received some institutional support from the MIT Media Lab, embodied a hacker ethos of constructing do-it-yourself sensing technologies and openly sharing information to ensure public safety and achieve political aims (PBS NewsHour, 2011). In many respects, Safecast operated through shared protocols to actualize a robust data commons, showing the empowering potential of participatory surveillance. At the same time, the practices of this network may signal an almost complete decline of trust in public institutions, such that the primary purposes may be ensuring self-protection through disaster preparedness and response, not necessarily dismantling risky infrastructures or challenging government truth claims about safety.

The project known as Crowd (Soft) Control offers another foray into empowering possibilities for participatory sensing. Based out of Northwestern University's AquaLab, researchers are designing mobile-phone applications to collect visual and sound data that are currently absent in databases because they exist at sites that are less frequently traversed by mobile phone users (Rula and Bustamante, 2012). For instance, urban sound maps that document sound-pollution hotspots may be skewed because they are populated primarily with data along main travel corridors, leaving less traveled routes underrepresented. Similarly, while personal and public image databases are replete with pictures of the front of buildings, there is a dearth of photographs of the side or rear of buildings, where exhaust fumes may be entering through air intake vents. In both of these situations, voids are left in the empirical record such that environmental problems may be unrecorded and therefore invisible within existing systems, making the likelihood of remediation slim. Crowd (Soft) Control seeks to build upon user familiarity with existing smartphone platforms, such as FourSquare or Facebook Places, to incentivize, through virtual rewards, the collection of missing visual and sound data. For instance, AquaLab researchers have devised a prototype for a game called "Ghost Hunter," wherein players must use their mobile phones to take photographs of supposed ghosts, who happen to be in locations where images are currently missing in existing databases (Rula and Bustamante, 2012). The intention of the researchers is to collect data that could assist with planning for urban sustainability, while drawing attention to environmental problems. User involvement is highly structured and constrained, so this would not necessarily constitute a democratic or truly participatory sensing system, but it does point to the possibility of progressive outcomes emerging from such projects.

Each of these alternative participatory sensing systems, as well as others like them (e.g., Chang, 2012; Monahan, 2010a; Ottinger, 2010; The Impact Project, 2012), offers a strong counterpoint to the controlling tone of security projects like Cell-All. Rather than rely on constructions of threats that invite restrictions of rights, neoliberal outsourcing, and the hardening of urban spaces, such alternatives operate in a register of "cosmopolitan security," which, as Stephen Graham has elaborated, is a mode of security that seeks to "address the real risks and threats that humankind faces in a rapidly urbanizing world prone to resource exhaustion, spiraling food, energy and water insecurity, biodiversity collapse, hyper-automobilisation, financial crises, and global warming..." (Graham, 2012: 326). That said, participatory sensing applications oriented toward cosmopolitan security still exist within states of extreme social inequality, so rather than being empowering in any universal way, they may instead highlight conditions of unequal exposure and invite conversations about persistent environmental racism and injustice (Monahan and Mokos, 2010). As with other forms of interactive surveillance, such systems also run the risk of being captured by commercial or security interests such that the data could be used for purposes that were not initially intended (Ellerbrok, 2011); thus, a certain amount of vigilance will be necessary to keep protocols open and directed toward social justice ends.

5. Conclusion

Crowdsourced sensing systems may drastically restructure spatial imaginaries as people learn to see and engage with heretofore largely hidden dimensions of urban spaces. While the design of these technological systems is contingent and currently open to varied outcomes, powerful security and industry players are asserting their influence to set overriding protocols that will ensure widespread ambient data collection, especially for security and commercial applications. In order to assess the politics of these emerging systems, this paper has mapped some of the institutional arrangements guiding technological development and analyzed the logics behind design decisions.

With DHS's Cell-All project, the vision for participation is one where members of the public act as passive data collectors for an almost completely closed system, where participants do not have access to data or environmental alerts beyond the individual level and where there are no opportunities for defining outcomes. The public, in this model, will be enticed or coerced to engage in the labor of being watched. This may happen through promises of protection from gas or chemical poisoning, through patriotic goals of averting mass casualties from terrorist attacks, or simply through invisible protocols that opt users in to data collection and sharing. At the same time, information systems are always embodied (Blanchette, 2012; Kitchin and Dodge, 2011), so as this version of participatory sensing grows, spatial protocols may emerge to sort and direct flows of individuals, perhaps giving priority access at security checkpoints or commercial venues to people voluntarily participating in the system—or singling out non-participants for added scrutiny or exclusion.

The Cell-All system also seeks to produce innovative organizational arrangements that advance research and development through public–private partnerships. DHS programs like Cell-All identify a narrow set of statistically unlikely scenarios, such as chemical attacks of public places or carbon monoxide poisoning, then frame problems in such a way that private-sector solutions are seen as the most reasonable and expedient. Viability for commercial success is measured through market research, and financial risks to participating companies are offset through DHS grants and assurances of a guaranteed market of government agencies and first responders upon project deployment. The program will produce data, which are viewed as being inherently positive. Industry partners stand to profit as well from vast repositories of personal data collected from millions of mobile phones, even if the uses of such sensor data are not yet defined.

Finally, by outsourcing privacy protections to companies and agencies implementing the systems, DHS both sidesteps responsibility for ensuring adequate protection of personal data and opens the field for industry partners to discover profitable uses for data. Privacy impact assessments, which may be required of security systems implemented by government agencies, are conducted only for the relatively innocuous development and testing phases of the project. In actual use, companies can collect data freely as long as they receive consent from users, such as in the form of license agreements that people routinely accept without reading (Böhme and Köpsell, 2010). The mission creep potentials of such surveillance systems are high. More than simply being a threat to privacy,

sensor data could lead to discrimination against individuals or groups who are perceived as living in risky environments or possessing risky lifestyles; precedents are already in place for such institutionalized forms of discrimination based on credit checks, drug tests, or health history, so sensor data from phones—were they readily available—could easily contribute to such practices.

Alternative participatory sensing systems offer templates for how environmental data could be collected in ways that are more democratic, encouraging of the development of user expertise, and dedicated to social and environmental justice. In short, the potential is there to harness such surveillance systems in the pursuit of cosmopolitan security and social equality (Graham, 2012). Because environmental threats are not distributed evenly, in order to achieve the progressive goals of their designers, such alternative systems must foster collective understandings of and responsibility for toxic exposure so that mitigation of risk will not be further individualized without altering the systems producing threats. If encoded in sociotechnical systems and practices, the cultivation of shared risk-topographies of environmental threats could serve as a powerful corrective to Cell-All's emphasis on individual responsibility, centralized control, and industry profits. That said, while some of these alternatives, like Safecast, are much more robust and functional at present than DHS's Cell-All, the restrictive technological protocols being established by DHS and its partners are creating a data enclosure that threatens to defer, perhaps indefinitely, the more laudable vision of a data commons.

References

Adey, P., 2006. 'Divided we move': the dromologics of airport security and surveillance. In: Monahan, T. (Ed.), Surveillance and Security: Technological Politics and Power in Everyday Life. Routledge, New York, pp. 195–208.

Akrich, M., 1992. The de-scription of technological objects. In: Bijker, W.E., Law, John (Eds.), Shaping Technology/Building Society: Studies in Sociotechnical Change. The MIT Press, Cambridge, MA, pp. 205–224.

Altheide, D., 2006. Terrorism and the Politics of Fear. Altamira Press, Lanham, MD.

Andrejevic, M., 2002. The work of being watched: interactive media and the exploitation of self-disclosure. Critical Studies in Media Communication 19 (2), 230–248.

Andrejevic, M., 2007. iSpy: Surveillance and Power in the Interactive Era. University Press of Kansas, Lawrence, Kan.

Andrejevic, M., 2011. The work that affective economics does. Cultural Studies 25 (4–5), 604–620.

Angell, M., 2004. The Truth about the Drug Companies: How They Deceive Us and What to Do About It. Random House, New York.

Associated Press, 2009. South Carolina: Ammonia Cloud Kills Woman. New York Times. <http://www.nytimes.com/2009/07/16/us/16brfs-AMMONIACLOUD_BRF.html> (accessed 17.09.12).

Barnard-Wills, D., 2012. Surveillance and Identity: Discourse, Subjectivity and the State. Ashgate, Burlington, VT.

Barrie, A., 2011. Smartphones Take on Silent Killers as Portable Danger Detectors. Fox News, September 29. <http://www.foxnews.com/tech/2011/09/28/cell-phones-take-on-silent-killers/> (accessed 17.09.12).

Blanchette, J.-F., 2012. Computing as if infrastructure mattered. Communications of the ACM 55 (10), 32–34.

Boddy, T., 2007. Architecture emblematic: hardened sites and softened symbols. In: Sorkin, M. (Ed.), Indefensible Space: The Architecture of the National Insecurity State. Routledge, New York, pp. 277–304.

Böhme, R., Köpsell, S., 2010. Trained to accept?: a field experiment on consent dialogs. In: CHI '10 Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, GA, pp. 2403–2406.

Bulkeley, W.M., 2009. Chicago's camera network is everywhere. The Wall Street Journal. <http://www.firetide.com/assets/0/112/138/9C3A795A-82DD-45CE-8BAD-6409B8BC8774.pdf> (accessed 16.09.12).

Center for Embedded Networked Sensing, 2008. Participatory Sensing, June 4. <http://www.youtube.com/watch?v=t-ltfpA3XiY> (accessed 17.09.12).

Chang, C., 2012. Mobile Air Quality. <http://candychang.com/mobile-air-quality/> (accessed 17.09.12).

Charmaz, K., 2006. Constructing Grounded Theory: A Practical Guide through Qualitative Analysis, second ed. Sage Publications, Thousand Oaks.

Clarke, R., 2009. Privacy impact assessment: its origins and development. Computer Law and Security Review 25 (2), 123–135.

Coaffee, J., 2004. Rings of steel, rings of concrete and rings of confidence: designing out terrorism in central London pre and post September 11th. International Journal of Urban and Regional Research 28 (1), 201–211.

Coaffee, J., Murakami Wood, D., Rogers, P., 2009. The Everyday Resilience of the City: How Cities Respond to Terrorism and Disaster. Palgrave Macmillan, Basingstoke, England.

Crang, M., Graham, S., 2007. Sentient cities: ambient intelligence and the politics of urban space. Information, Communication and Society 10 (6), 789–817.

Cuff, D., Hansen, M., Kang, J., 2008. Urban sensing: out of the woods. Communications of the ACM 51 (3), 24–33.

Curry, M.R., Phillips, D.J., Regan, P.M., 2004. Emergency response systems and the creeping legibility of people and places. The Information Society 20, 357–369.

Dennis, S., 2011. Cell-All Program Overview. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Ellerbrok, A., 2011. Playful biometrics: controversial technology through the lens of play. The Sociological Quarterly 52 (4), 528–547.

Finn, R.L., Wright, D., 2012. Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Computer Law and Security Review 28 (2), 184–194.

Fisher, J.A., 2009. Medical Research for Hire: The Political Economy of Pharmaceutical Clinical Trials. Rutgers University Press, New Brunswick, NJ.

Fussey, P., Coaffee, J., Armstrong, G., Hobbs, D., 2011. Securing and Sustaining the Olympic City: Reconfiguring London for 2012 and Beyond. Ashgate, Burlington, VT.

Gilliom, J., Monahan, T., 2013. SuperVision: An Introduction to the Surveillance Society. University of Chicago Press, Chicago.

Graham, S., 2010. Cities Under Siege: The New Military Urbanism. Verso, London.

Graham, S., 2012. Digital medieval. Surveillance and Society 9 (3), 321–327.

Graham, S., Wood, D., 2003. Digitizing surveillance: categorization, space, inequality. Critical Social Policy 23 (2), 227–248.

Haggerty, K.D., Ericson, R.V., 2006. The new politics of surveillance and visibility. In: Haggerty, K.D., Ericson, R.V. (Eds.), The New Politics of Surveillance and Visibility. University of Toronto Press, Toronto, pp. 3–25.

Hoffman, D., 2011. Qualcomm Project Presentation. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

King, M., Bailey, C., 2007. Carbon monoxide – related deaths in the United States, 1999–2004. Morbidity and Mortality Weekly Report (CDC) 56 (50), 1309–1312.

Kitchin, R., Dodge, M., 2011. Code/Space: Software and Everyday life. MIT Press, Cambridge, MA.

Klauser, F.R., 2010. Splintering spheres of security: Peter Sloterdijk and the contemporary fortress city. Environment and Planning D: Society and Space 28 (2), 326–340.

Klauser, F.R., Ruegg, J., November, V., 2008. Airport surveillance between public and private interests: CCTV at Geneva International Airport. In: Salter, M.B. (Ed.), Politics at the Airport. University of Minnesota Press, Minneapolis, pp. 105–126.

Koskela, H., 2010. 'Did you spot an alien?' Voluntary vigilance, borderwork and the Texas Virtual Border Watch Program. Space and Polity 14 (2), 103–121.

Li, J., 2011. Nanosensor-Cellphone Integration for Extended Chemical Sensing Network. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Lianos, M., Douglas, M., 2000. Dangerization and the end of deviance. British Journal of Criminology 40 (2), 261–278.

Lyon, D., 2001. Surveillance Society: Monitoring Everyday Life. Open University, Buckingham, England; Philadelphia.

Lyon, D., 2003. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. Routledge, New York. <http://www.loc.gov/catdir/enhancements/fy0650/2002075104-d.html>.

Magnet, S., 2011. When Biometrics Fail: Gender, Race, and the Technology of Identity. Duke University Press, Durham.

Monahan, T., 2010a. Surveillance as governance: social inequality and the pursuit of democratic surveillance. In: Haggerty, K.D., Samatas, M. (Eds.), Surveillance and Democracy. Routledge, New York, pp. 91–110.

Monahan, T., 2010b. Surveillance in the Time of Insecurity. Rutgers University Press, New Brunswick.

Monahan, T., Mokos, J.T., 2010. Sensing environmental danger in the city. International Review of Information Ethics 12, 21–27.

Monahan, T., Palmer, N.A., 2009. The emerging politics of DHS fusion centers. Security Dialogue 40 (6), 617–636.

Montagnino, J., 2012. NC4 Situational Readiness Solutions to Manage Risks. <http://www.nc4.us/> (accessed 09.09.12).

Murakami Wood, D., 2007. Pervasive Surveillance: Enabling Environments or Embedding Inequalities. Workshop on Surveillance and Inequality. Arizona State University.

Murakami Wood, D., 2009a. Chicago: The Future of US CCTV? Notes from the Ubiquitous Surveillance Society. <http://ubisurv.wordpress.com/2009/02/21/chicago-the-future-of-us-cctv/> (accessed 07.06.11).

Murakami Wood, D., 2009b. Where Will the Big Red Balloons Be Next? Notes from the Ubiquitous Surveillance Society. <http://ubisurv.wordpress.com/2009/12/04/big-red-balloon/> (accessed 16.09.12).

Murakami Wood, D., Webster, C.W.R., 2011. The normality of living in surveillance societies. Innovating Government 20 (3), 151–164.

Needs, C., 2011. NC4 Project Presentation. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Neighborhood Link, 2010. How Landlords Can Use Credit Scoring to Make Rental Decisions. <http://www.neighborhoodlink.com/article/Homeowner/Credit_Scoring_Rentals> (accessed 19.07.11).

O'Harrow, R., 2005. No Place to Hide. Free Press, New York.

Ottinger, G., 2010. Constructing empowerment through interpretations of environmental surveillance data. Surveillance and Society 8 (2), 221–234.

PBS NewsHour, 2011. Safecast Draws on Power of the Crowd to Map Japan's Radiation, November 10. <http://www.pbs.org/newshour/bb/science/july-dec11/japanradiation_11-10.html> (accessed 17.09.12).

Rula, J., Bustamante, F.E., 2012. Crowd (soft) control: moving beyond the opportunistic. In: Proc. of the Thirteenth Workshop on Mobile Computing Systems and Applications (HotMobile), San Diego, CA.

Safecast, 2012. Safecast. <http://blog.safecast.org/> (accessed 17.09.12).

Shilton, K., 2009. Four billion little brothers?: privacy, mobile phones, and ubiquitous data collection. Communications of the ACM 52 (11), 48–53.

Shilton, K., 2012. Participatory personal data: an emerging research challenge for the information sciences. Journal of the American Society for Information Science and Technology 63 (10), 1905–1915.

Synkera Technologies, 2011. Chemical Sensors for Mobile Devices. <http://www.synkera.com/sensors/chemical-sensors-for-mobile-devices.html> (accessed 19.09.12).

The Impact Project, 2012. Trade, Health and Environment Impact Project. <http://theimpactproject.org/index.html> (accessed 17.09.12).

Thrift, N., French, S., 2002. The automatic production of space. Transactions of the Institute of British Geographers 27 (4), 309–335.

U.S. Department of Homeland Security, 2007. Cell-All Ubiquitous Biological and Chemical Sensing. <https://http://www.fbo.gov/index?s=opportunity&mode=form&id=f292c1fdbd46777a3ff8ca64ef96658f&tab=core&_cview=1> (accessed 17.09.12).

U.S. Department of Homeland Security, 2010. Cell-All: Super Smartphones Sniff Out Suspicious Substances. <http://www.dhs.gov/cell-all-super-smartphones-sniff-out-suspicious-substances> (accessed 17.09.12).

U.S. Department of Homeland Security, 2011a. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

U.S. Department of Homeland Security, 2011b. Privacy Impact Assessment for the Cell All Demonstration. <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_s&t_cell_all.pdf> (accessed 19.09.12).

U.S. Department of Homeland Security, 2011c. Transcript of the Meeting of the Data Privacy and Integrity Advisory Committee. May 19. <http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy_dpiactranscript_may192011mtg.pdf> (accessed 17.09.12).

Verrico, J.S., 2011. Welcome and Opening Remarks. Cell-All Live Demonstration for Environmental Sensing (Webcast), September 28. <http://cellall.webcaston.tv/home/homepage.php> (accessed 17.09.12).

Wall, T., Monahan, T., 2011. Surveillance and violence from afar: the politics of drones and liminal security-scapes. Theoretical Criminology 15 (3), 239–254.

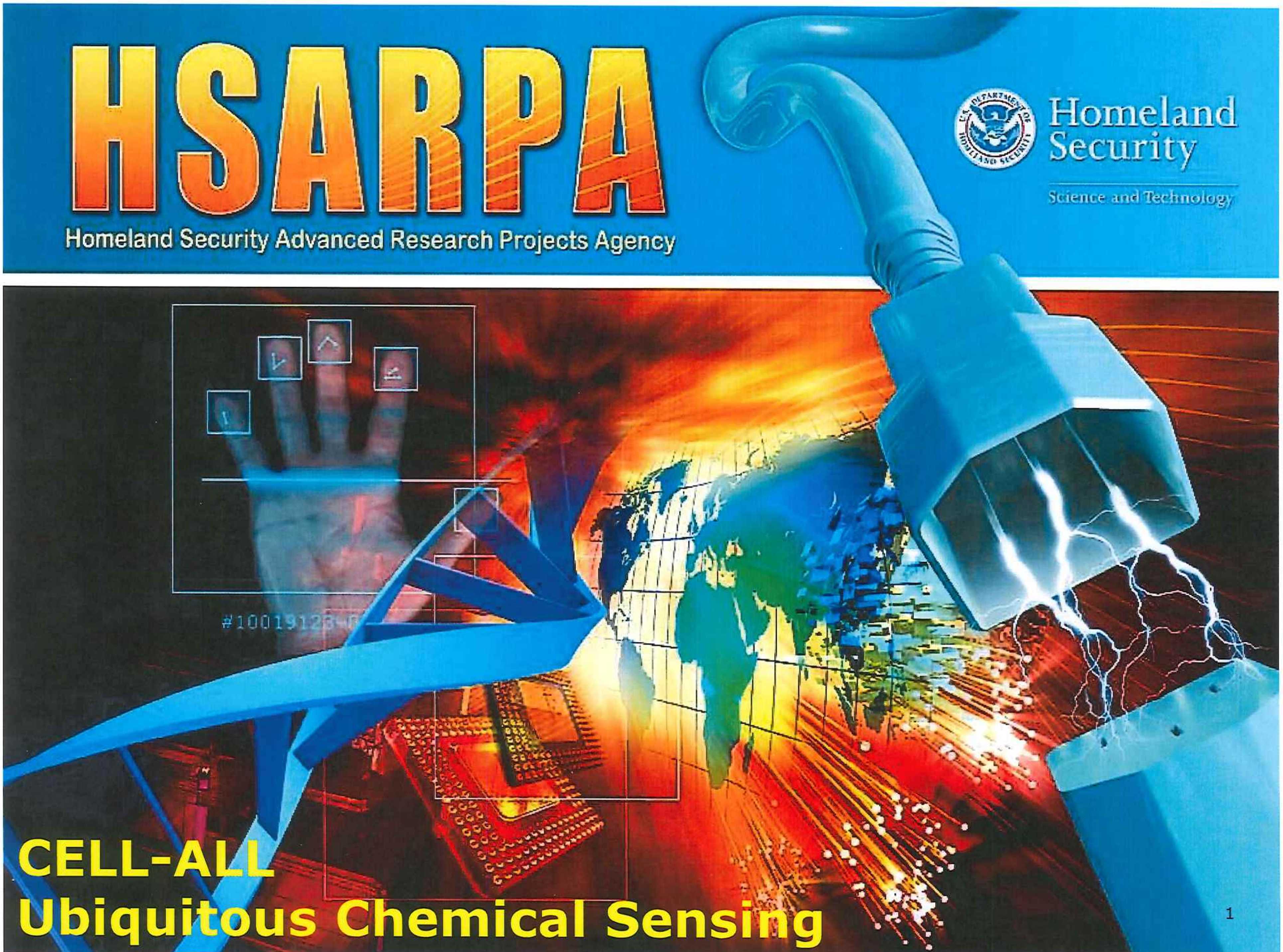
Weber, J., 2011. Techno-security, risk and the militarization of everyday life. In: Conference on "The Computational Turn: Past, Presents, Futures?". Aarhus University, pp. 168–173.

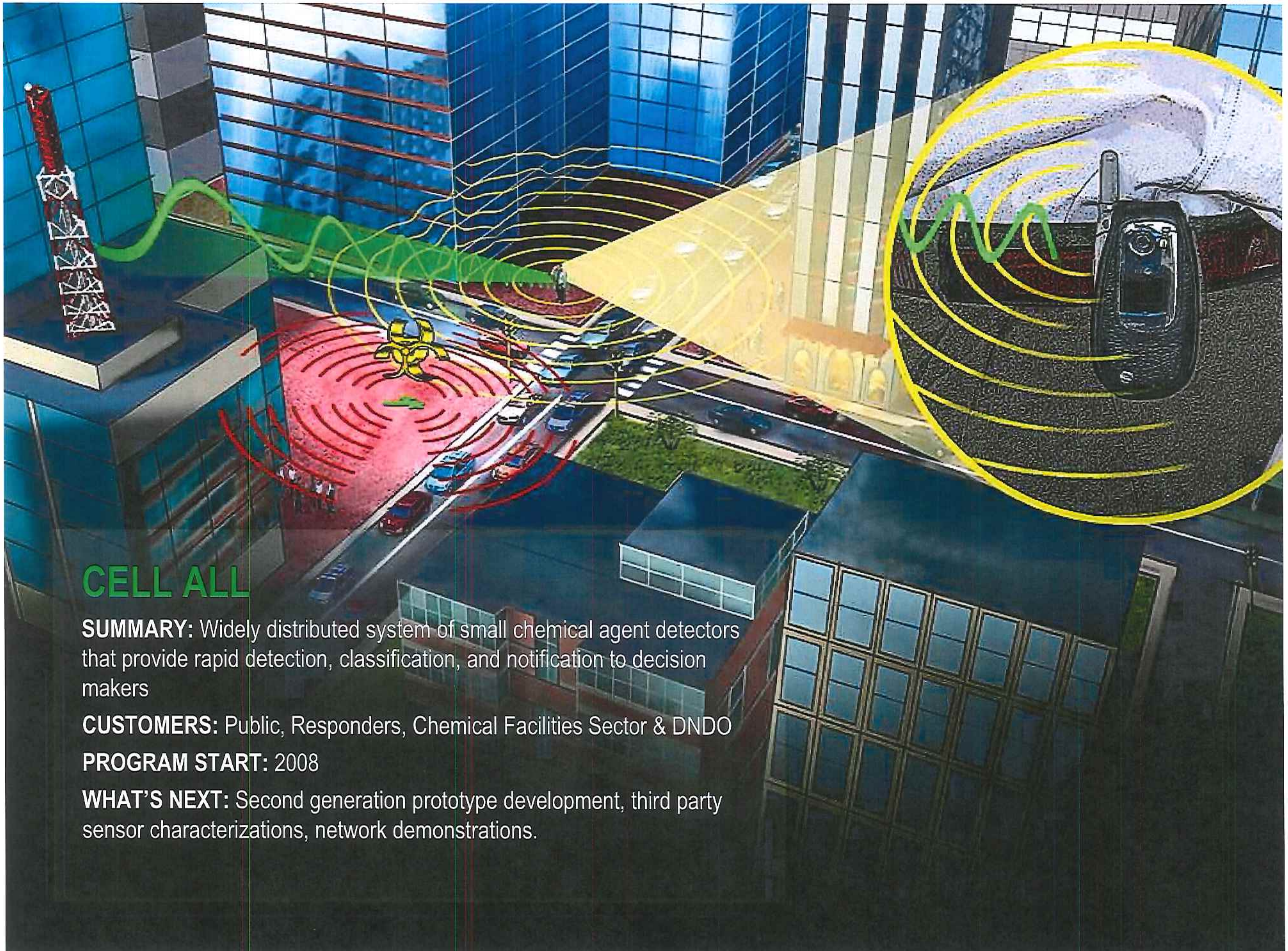
Whitson, J.R., Haggerty, K.D., 2008. Identity theft and the care of the virtual self. Economy and Society 37 (4), 572–594.

Winner, L., 1986. The Whale and the Reactor: A Search for Limits in an Age of High Technology. University of Chicago Press, Chicago.

Woodhouse, E., Hess, D., Breyman, S., Martin, B., 2002. Science studies and activism: possibilities and problems for reconstructivist agendas. Social Studies of Science 32 (2), 297–319.

EXHIBIT 5


HSARPA
Homeland Security Advanced Research Projects Agency
Homeland Security
Science and Technology
CELL-ALL
Ubiquitous Chemical Sensing
1


CELL ALL
SUMMARY: Widely distributed system of small chemical agent detectors that provide rapid detection, classification, and notification to decision makers
CUSTOMERS: Public, Responders, Chemical Facilities Sector & DNDO
PROGRAM START: 2008
WHAT'S NEXT: Second generation prototype development, third party sensor characterizations, network demonstrations.

Cell-All Goals

Homeland Security Goals (QHSR)

Mission 1: Preventing Terrorism and Enhancing Security

- Goal 1.1: Prevent Terrorist Attacks
- Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities

Mission 5: Ensuring Resilience to Disasters

- Goal 5.1: Mitigate Hazards
- Goal 5.2: Enhance Preparedness
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Rapid Recovery

S&T Goals

- Rapidly develop and deliver knowledge, analysis, and innovative solutions that advance the mission of the Department

HSARPA Goals

  - Proof of concept technology development and demonstration
  - Potential for significant gains in technical capability

Homeland Security

Motivations to Improve Detection

Large, expensive and stationary systems represent state of the art for chemical agent detection

A variety of less expensive handheld systems are available as separate systems

Geographic coverage is limited to specific areas for each deployment

Sampling may not reflect the environment where people are actually located

Homeland Security

Approach

Create a large and dynamic sensing system

- Miniaturized and effective sensing capability
- Integrate low-cost sensing into common devices
  - Sensing becomes part of the environment
- Harvest the benefits of network effects and crowd sourcing
- Privacy Protection for individuals
- Integrate with 261 million cell phones now used in the U.S.
- Leverage billions of dollars spent each year in sensor, carrier network and cell phone development

Gain earlier indications and warning for hazardous chemical events

Homeland Security

Technical Approach

Embedded Miniature Sensors

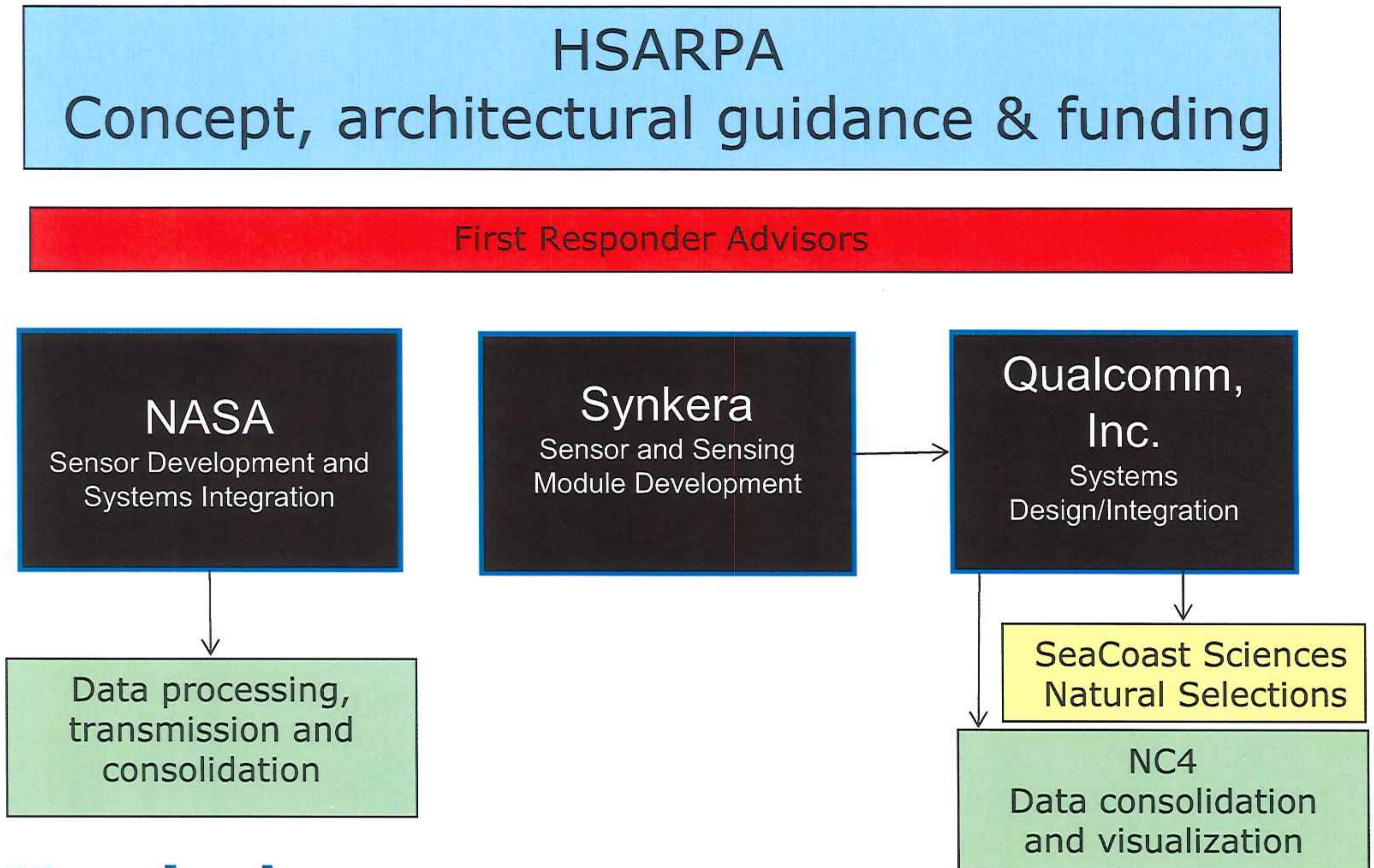
- Sample collection
- Reusable devices with lifetimes that equal that of the host device
- Address sensor sensitivity & selectivity in the environment
- Prototype concepts for integrated sensing
- Methods for read/report of sensor information

Sensing Network to Significantly Expand Coverage

- Investigate sensor performance in a large scale networks
- Concepts of Operation for ubiquitous sensing
- Modeling large scale system characteristics and response

Homeland Security

CellAll Team



Homeland Security

Performers

NASA Ames Research Center

Developed a world smallest and ultra low power nanosensor array module with sensors, a sampling device and a data acquisition board all-in-one (a stamp size) integrated with an iPhone and an app for data processing and transmission

Qualcomm

State-of-the-art miniaturized detection system integrated into Android cell phones

Synkera

Sensor & Module Developer

Homeland Security

Phase 1 – Proof of Concepts

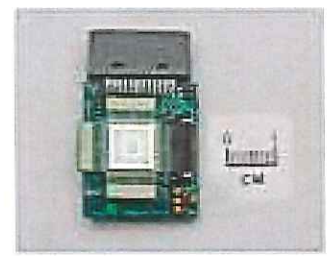
- Establish miniature sensor efficacy
- Discover limitations for cell phone integration
- Develop first generation prototypes
- Proof of concept demonstrations
  - NASA – Leveraging nanosensor work for space missions to further miniaturizing the space qualified integrated sensing system for detection of toxics and CWAs using smartphones.
  - Synkera – Leveraging SBIR funded development of miniature sensors.
  - Qualcomm – Using an existing hardware platform to integrate an existing sensor and demonstrate its ability to sense a defined set of agents

Homeland Security

Phase I Prototypes

Qualcomm FFA

NASA ARC nanosensor module for iPhone integration



iPhone Specifications

Homeland Security

Phase II Prototypes

- Achieve a greater number of total prototype devices at a reasonable unit cost
- Sensor data transmission via 3g and/or Wi-Fi
- Multiple sensors network for chemical profiling
- Decouple the chemical sensor from the phone.
- Multiple sensor units per phone are possible
- Bluetooth/Proprietary Interfaces
- Standardize the sensor platform
- Increase opportunities for participation

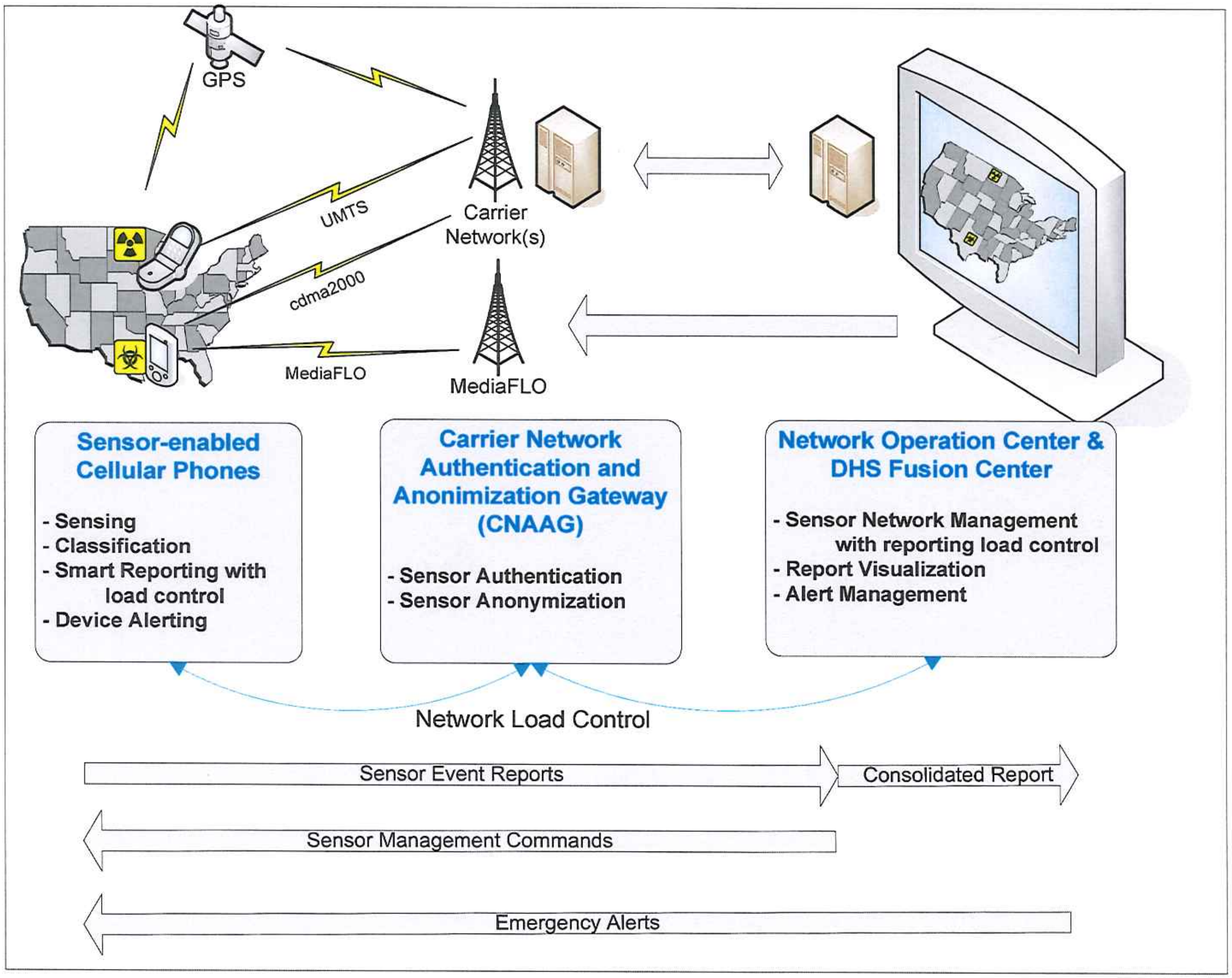
Homeland Security

Summer 2011 Demonstrations

- LAFD, Frank Hotchkins Memorial Training Center
  - Carbon Monoxide
  - Personal Protection Scenario
  - Audio Alarm
  - In Case of Emergency (ICE) Alerts
- FEMA, Center for Domestic Preparedness
  - Toxic Chemical Agents
  - Hazardous Materials Response Team Scenario
  - Network response
  - Geographic-based visualization

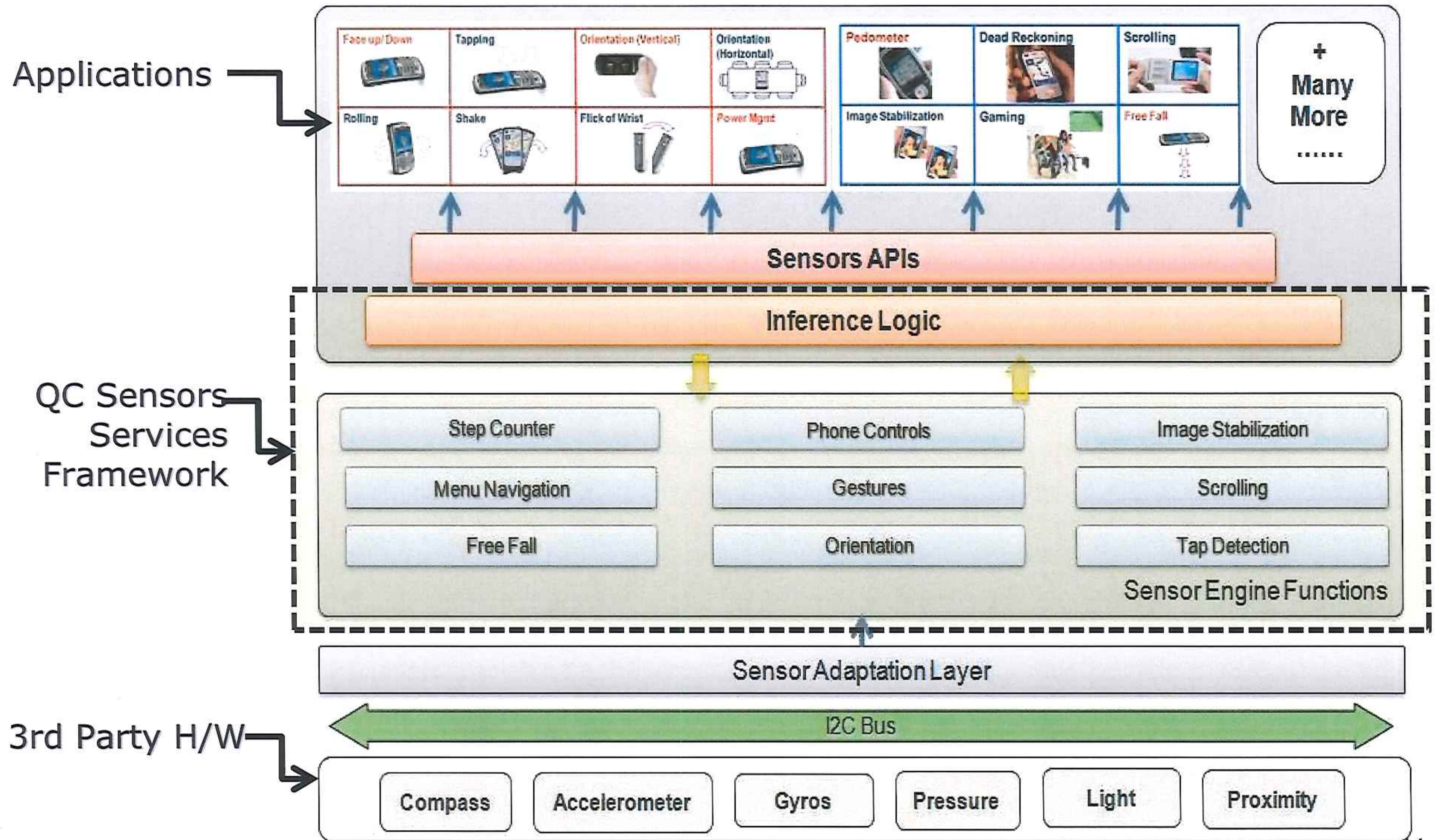
Homeland Security

Network control and architecture



QUALCOMM **QUALCOMM** Government Technologies

Sensors Services Framework – Approach



Cell Phone Environment

- Handsets are very price sensitive
- Components must be small and thin
- Battery life is a key benchmarks and more is better
- Short development time
- Short life cycle
- No time for redesigns
- Must be adaptable to standard manufacturing processes
- Temperatures/humidity/pressure fluctuate (Polar to Equator externally)
- RF interference issues
- Applications must be thin
- Algorithms must be efficient
- False positives will make this fail

More details

- Cost
  - Features like this usually require component cost of <$1.00 (including support sensors for humidity, pressure and temperature if necessary)
  - Studies indicate
    - Consumers might be willing to pay the additional cost of $1.00
    - A personal sensing application for CO may improve up take
    - False positives would kill feature quickly
  - The cost associated with the manufacturing process is equally important
    - OEMs cannot be expected to calibrate (self calibration)
    - Must use a standard operating system

More details

- Digital Interfaces
  - UART (up to 4Mbps)
    - Two wire interface (Transmit/Receive)
    - Supporting asynchronous data
  - I2C (typically used for sensors)
    - Used for command and control of devices such as the camera
    - Two wire Master/Slave type bus
    - Clock line and data line
    - Supports 1 Master and multiple Slaves
    - Generally supports 100KHz and 400KHz operation on the bus
  - Analog
    - Some handsets support this
    - Typically used for temperature
    - May offer integration advantages

More details

- Manufacturing Consideration
  - Manufacturing temperatures as high as 260° C possible
    - A flex circuit or socket approach may be necessary
  - Size
    - 3-15 sensors on a <6x6x2mm optimally 2x2x1mm
    - Including components necessary for support (fans, vents, filters, dwell)
  - Packaging - must withstand the vibration, drops and abuse of a typical handset
  - Software – must be release controlled & compatible with the an existing operating system

More details

- Power
  - Many power supplies operating at different voltages
  - Both linear and switching
  - Batteries 3.7V nominal, 3.2-4.2V range
  - Charged using linear charging from a 5V supply

Sample Sensor Supply voltages

Symbol	Parameter	Min	Typ	Max	Units
Vcc	Sensor Analog Circuit supply voltage	+2.85	+3.0	+3.15	V
Vdd_io	Sensor Digital I/O voltage	+1.62	+2.6	+3.63	V

Sample Current Goals

Symbol	Parameter	Min	Typ	Max	Units
Active	Sensing	-	5mA	-	mA
Standby	Standby	-	10uA	-	uA
Sleep	Sleep	-	1uA	-	uA

EXHIBIT 6

The Government's "use" of Plaintiff's CMDC device that was: solicited by the Government; funded by the Government; manufactured for the Government; and, used by the Government; is not "*Incidental Use*" by the Government

NODE+ Platform Integrates Sensors with Smartphones

Consumer Goods

NASA Technology

In 2007, when the Department of Homeland Security (DHS) issued a call for a sensor that could equip a smartphone with the ability to detect dangerous gases and chemicals, Ames Research Center scientist Jing Li had a ready response. Four years earlier, she led a team that wrote a paper on the use of carbon nanotube sensors for gas and organic vapor detection, which would later receive Ames' 2012 H. Julian Allen award for outstanding science and engineering papers.

She had been developing the use of single-walled carbon nanotubes that respond to various gases and compounds for use in NASA applications, such as evaluating planetary atmospheres, detecting chemicals around rocket launch pads, and monitoring the performance of life-support systems. Her proposal in response to DHS's Cell-All initiative was awarded funding through an interagency agreement in 2008. What she still needed was a way for the device to "sniff" the air for samples and a system that would allow it to interface with a smartphone.

The NODE platform can be outfitted with an array of different sensor modules for detecting light, gases, temperature, motion, and more. It can store data or transmit it to a smart device using Bluetooth wireless technology.

Li approached George Yu of Genel Systems Inc. "Genel had the technology to provide a very small sample collection system," Li says, noting that the company was subcontracted shortly after funding was awarded. In the end, however, that sampling jet proved too noisy, and Li and her team settled instead on a tiny fan. Then a separate contract for the cell phone interface system fell through. "That contract didn't work out, so I asked George to do it—I know he is good at electrical circuit design," Li says.

The team settled on the iPhone, which was new at the time, and Li convinced the program manager at DHS that the sensor should be a module attached to the outside of the phone, rather than a system built into the phone's guts. "This is a very new technology, and there will be a lot of iterations. Making it interchangeable will make it easier to update," she explains.

This modular design not only will pave the way for future smartphone chemical sensors but also presaged the line of interchangeable, smartphone-savvy sensors Yu would commercialize a few years later, after founding Variable Inc. in Chattanooga, Tennessee.

Yu figured out how the sensor module could draw its power from the cell phone battery and use the phone to digitally process the data it gathered and transmit it to a central location, such as a cloud

platform. Most of the design for the microprocessor, memory, communication protocol, back-end Web structure, data storage, and cloud technology he developed for NASA and DHS under a NASA subcontract would later appear in Variable's NODE wireless sensor platform.

The NODE+ platform, shown here attached to the bicycle handlebars in the bottom left, tracks motion with a gyroscope, accelerometer, and magnetometer. It can also let a whole host of other sensors—up to two at a time—communicate with smart devices.

Ultimately, Li's team outfitted each of 40 iPhones with a tiny chip containing 32 carbon nanotube sensors that react to potentially harmful chemicals, such as ammonia, nitrogen dioxide, hydrogen chloride, and chlorine, as well as volatile organic compounds, such as benzene and toluene. Most of the phones have been delivered to DHS and are being tested by technical first responders and trained personnel.

"DHS wants to utilize chemical detection technology incorporated with a cell phone to do global or regional chemical detection," Li says. If firefighters arrive at a scene involving a toxic gas leak, for example, the device can let individuals know how far into the area they can safely go, and the collective data from multiple firefighters carrying the technology can map the extent and boundary of the chemical hazard. "Then they can make decisions based on the detection results at certain locations," says Li. All this is accomplished without requiring anyone to carry an additional device—in almost all cases users are carrying cell phones anyway.

"It became immediately clear that this integration of nanosensor technology in combination with a cell phone is extremely powerful," Yu says. To launch his commercial line, however, he began with simpler technology.

Technology Transfer

Building on the integration system he developed for the Cell-All initiative, Yu developed his NODE platform—a cylinder not much bigger than a man's thumb that can transmit data from sensors to a smartphone or other smart device and that also has its own memory port capable of storing data to be uploaded to any computer. Unlike the sensor developed for DHS, NODE operates independently of the cell phone and transmits the data to the phone or other device using Bluetooth wireless technology.

The NODE Chroma color sensors let the user upload a custom color set and reference colors against a library of hues.

Variable converted off-the-shelf sensors, such as infrared thermometers, color referencers, motion sensors, and barcode readers, into interchangeable modules that can be snapped onto either end of NODE, so it can use two modules simultaneously. Echoing the Cell-All project, there is a module for carbon dioxide detection and another that senses carbon monoxide, nitric oxide, nitrogen dioxide, chlorine gas, sulfur dioxide, and hydrogen sulfide. Another module measures ambient light, room temperature, humidity, and barometric pressure.

"Using a common platform for multiple sensor modules, you save a lot of money through economies of scale," Yu says.

The product line went on the market in 2012, and by summer of 2014, it was already in its second generation, NODE+, which Yu says is faster, uses less power, is more durable, has more memory, and is compatible with Android devices as well as Apple smart devices.

Benefits

Yu says the sensors have found extensive use in the areas of supply-chain management, transport, and logistics.

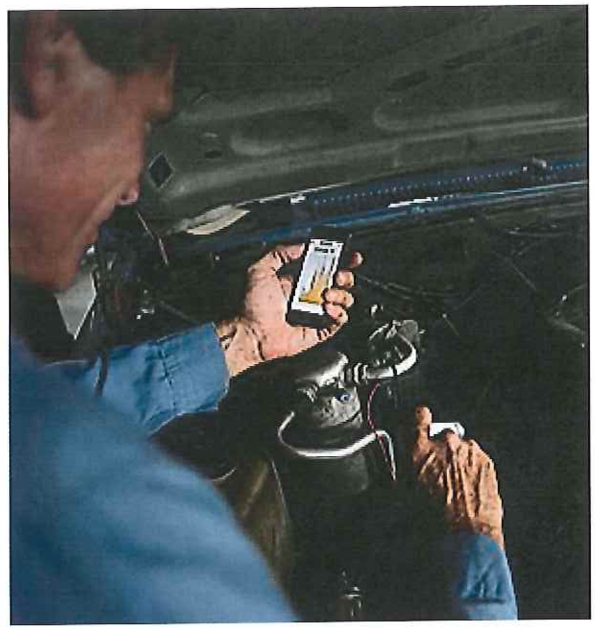
An early adapter of the technology was the pharmaceutical industry. "Their packages are extremely high-value, and the cost of shipping penicillin across the country is so high that this type of sensing device is of huge value for them," Yu says, noting that a sensor embedded in a package can record temperatures and vibrations and then report that information to a smartphone.

A company that deals with paints or other color-specific products can use one of the Chroma sensors for quality control, just as one that deals with food can use the infrared thermometer or thermocouple probe for temperature assurance.

"As we started deploying this product, we got a huge amount of feedback from our customers," Yu says, adding that the response resulted in, among other developments, the suggested pairings of sensors on the company's Web site. Since each NODE can house two sensors, someone doing temperature control, for example, can take a temperature reading and then flip the device around to scan a product barcode that would show which product the reading applies to.

All the data can be automatically recorded on the accompanying smart device, saving time and cutting down on user error.

"Variable is also a solutions partner for the 'Internet of things,'" says Alex Lavidge, the company's vice president of business development and marketing. "We use NODE+ as a platform to gather market intelligence from our clients and innovation partners. From these studies, we determine how we can integrate mobile sensor features in the future that add the most value for targeted segments in both the private and public sectors." Lavidge says a lot of these trials are currently centered around integrating sensors with wearable technology like smart safety goggles, as well as other sensor hardware concepts that can be integrated with big data analytics platforms to help end-users make "smarter decisions faster."



NODE's Therma modules detect temperature at a distance and have proven popular in the food service, auto repair, manufacturing, and home inspection industries.

To solicit further input, in the summer of 2014, Variable held its international Hackanode challenge, offering a total of $16,500 in prizes in various categories to developers who build or integrate existing sensor functions with the NODE+ platform using their own apps. Among the 10 judges were Apple cofounder Steve Wozniak and Tom Suder, president of the mobile Government technology organization Mobilegov.

Even before the contest, independent developers had created numerous apps for the platform.

It has also received widespread attention within the computer and technology industries. CNN Money magazine called NODE the coolest gizmo found at the Consumer Electronics Show 2013, and the company was named Most Innovative Startup at that year's Southland technology and entrepreneur conference. NODE was a finalist in the Spark Awards' 2013 International Design Competition, the Made in the USA category of Walmart's 2013 Get on the Shelf competition, and the Tech for a Better World category at the 2014 Consumer Electronics Show.

Variable now has 25 employees, about a third of whom are manufacturers. The devices are built right in Chattanooga.

Yu says the company is now working to incorporate the sort of nanotube sensor technology he integrated with iPhones during his work with Li.

Li says she, too, hopes to develop her sensors to the point that the price can be brought down enough to make them viable consumer products.

"Hopefully we can continue this work, because this technology can be used for many application areas, like industrial, environmental, and in space," she says.

Previous Page / Home / Contents / Next Page

The Government's "use" of Plaintiff's CMDC device that was: solicited by the Government; funded by the Government; manufactured for the Government; and, used by the Government; is not "Incidental Use" by the Government

1. The U.S. Government Accountability Office: According to the most recent OMB estimate, the federal government spends about $1.2 billion annually on about 1.5 million mobile devices and associated services. View GAO-15-431. For more information, contact Carol R. Cha at (202) 512-4456 or chac@gao.gov.

2. Beginning in year 2008 and continuing, the "Government" has given authorization and consent through contracts, agreements, grants, and procurements, to at least the mobile device manufacturers and developers of Apple, Samsung, Qualcomm, LG, Motorola, and Panasonic for the development and manufacture of mobile devices to be used by and for the "Government". All contracts, agreements, and procurements were made with the mobile device manufacturers Apple, Samsung, Qualcomm, LG, Motorola, and Panasonic after the Patent Owner gave notice to the "Government" between the years 2006 and 2007. See Plaintiff's discovery production at Section VII., A-E; and Docket No. 101 for the following:

3. 2008: "DHS S&T is pursuing what's known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes." Quote taken directly from the Department of Homeland Security's website.

4. 2008: "During the demonstration, chemical readings captured from the simulated scenarios as well as location data are transmitted to the test network. The cell phone

number is also transmitted; however, this information is scrubbed by the cell phone provider (per agreements with S&T) and is not displayed in the final output."

5. 2012: "The U.S. Department of Defense expects in coming weeks to grant two separate security approvals for Samsung's Galaxy smartphones, along with iPhones and iPads running Apple's latest operating system—moves that would boost the number of U.S. government agencies allowed to use those devices. An approval by the Pentagon is considered as the highest standards in security."

6. 2013: Smartphones and Handheld Devices for Defense and Homeland Security Strategies, Plans, Challenges & Opportunities Symposium:

a. "U.S. Coast Guard Smartphones Needs, Challenges & Opportunities" Rear Admiral Robert E. Day, Jr., Assistant Commandant for Command, Control, Communications, Computers & Information Technology, (C4IT) & Director, Coast Guard Cyber Command, Pre-Commissioning Detachment, U.S. Coast Guard.

b. "DoD Mobile Strategy" Mr. Mark Norton, Senior Engineer, Department of Defense, Office of the Chief Information Officer, Office of the Under Secretary of Defense (CIO/OSD).

c. "Update on Spectrum Sharing for Mobile Devices at the Tactical Edge" Mr. Julius Knapp, Chief Engineer, Office of Engineering and Technology, Federal Communications Commission (FCC).

d. "Secure Smartphone Computing, Needs and Opportunities for a Secure yet Mobile Platform" Mr. Keith Trippie, Executive Director, Enterprise System

Development, Office of the Chief Information Officer, Department of Homeland Security (DHS).

e. "DISA's Strategic Mobility Vision" Mr. Gregory Youst, Chief Mobility Engineer, Technology and Integration Division, Chief Technology Officer, Defense Information Systems Agency (DISA) (invited).

f. "Content-Based Mobile Edge Networking (CBMEN)" Dr. Keith Gremban, PhD., Program Manager, Content Based Mobile Edge Networking (CBMEN), Defense Advanced Research Project Agency (DARPA).

g. "Transformative Apps Program" Mr. Doran Michaels, Program Manager, Transformative Apps, DARPA.

h. "Windshear II Update" Mr. John-Isaac Clark, Chief Innovation Officer, Thermopylae Sciences & Technology & Mr. Lenwood Washington, Senior Systems Engineer, Mission Integration Directorate, Acquisition and Engineering, National Reconnaissance Office (NRO).

i. "Advancements in Mobile Devices for Chem-Bio Detection and Characterization" Dr. Calvin CHUE, PhD., Research Biologist, U.S. Army Research, Development and Engineering Command (RDECOM).

j. "ADAPT Unattended Ground Sensor Using Android Operating System and Original Design Manufacturers" Mr. Mark Rich, Program Manager, Strategic Technology Office, DARPA.

7. 2013: "The U.S. Department of Defense confirmed in a statement on Friday that Apple's iOS 6 mobile operating system is secure enough to connect to secure Pentagon networks."

8. 2013: “Samsung's potential government deal signals new era for mobile security: Samsung may be ready to sign deals with the FBI and the U.S. Navy. Analysts say the news is proof that mobile in the enterprise has arrived. Samsung is close to inking a deal with the FBI and the U.S. Navy for mobile devices.”

9. 2013: “National Institute of Standards and Technology (NIST), which examines and tests mobile devices and technologies for security clearance, granted the Apple software FIPS 140-2 certification (Level 1) last Friday. This approves iPhones and iPads running the software in conjunction with the U.S. government's lowest level of national security clearance.”

10. 2013: “The U.S. Department of Defense announced today that it was further dropping its exclusive BlackBerry contract and opening all of its mobile communications networks to Apple, Google, and other device makers. ‘The Department of Defense is taking a leadership role in leveraging mobile device technology by ensuring its workforce is empowered with mobile devices,’ Defense Department Chief Information Officer Teri Takai said in a statement today.”

11. 2013: “Samsung recently received the nod from the Pentagon for any Samsung device protected by the Knox security software, which includes the Galaxy S4 and other compatible tablets.”

12. 2013: “For the first time, Apple's push into federal use opens up the U.S. government and military to competition for device procurement in the mobile space.”

13. 2014: “The mobile device management system–MDM–began operating Jan. 31as a control system through which approved devices must operate to get access to Defense

Department networks. The MDM enforces security policies by blocking or permitting certain functions on smartphones and tablets."

14. 2014: "By opening its networks to Samsung and Apple devices, Defense Information Systems Agency (DISA) intends to broaden the variety of mobile computers that troops and civilian Defense Department employees can use in the field, on bases, in offices and elsewhere to receive and send information and work almost anywhere at any time."

15. 2014: "Samsung has announced that five of its Galaxy devices have been approved for the U.S government's Defense Information System Agency (DISA) products list. The devices include the Galaxy S4, Galaxy S4 Active, Galaxy Note 3, the Galaxy Note Pro 12.2 and the Galaxy Note 10.1 2014 Edition. All of them are using Android 4.4 (KitKat) along with Samsung's KNOX secure workspace platform, which includes system-level encryption for enterprise-based apps."

16. 2014: "The United States Air Force is replacing 5000 legacy BlackBerry smartphones with Apple's iPhone, and eventually all of their BlackBerry users will have to make the changeover. The announcement, reported by Defense News, comes as the future of BlackBerry within the Department of Defense is debated, with the chips seeming to fall on the side of transitioning away from a network supporting a mish-mash of BlackBerry 6 and 7 devices to a mix of modern devices — though apparently without BlackBerry 10 in that mix."

17. 2015: "Navy Plans for Android and iOS Devices. The Navy Enterprise Networks (NEN) Program Office is making progress on plans to transition to more modern mobile devices. Early users will be able to choose between the iPhone 5c and 5s, but the Navy wants to be as flexible as possible and allow users to pick the devices that will work best for them, and plans to approve a wider range of devices. Approval to use the iPhone 6 and iPad Air

is expected in Jan. or Feb. 2015, and approval to use Samsung Android phones and tablets is expected in March."

18. 2016: "This fiscal year Marines will receive Samsung smart phones that make calling for fire support easier, quicker and more accurate. The Target Handoff System Version 2, or THS V.2, is a portable system designed for use by dismounted Marines to locate targets, pinpoint global positioning coordinates and call for close air, artillery and naval fire support using secure digital communications."

19. 2016: "Both the LG Electronics G5 and V10 received a security certification from the U.S. Defense Information Systems Agency, as well as a certification by the National Information Assurance Partnership, which administers independent tests to see if the devices are reliable and secure. The two newer LG smartphone models have joined the select list of official devices that can be used by Department of Defense employees, according to the handset manufacturer and a DOD website. LG's older models, the G3 and G4 also received DISA certifications. The phones come equipped with LG's encryption technology from 2013, LG GATE. The advanced tech has secure email options, supports Virtual Private Network (VPN), and can remotely wipe the phone's memory."

20. 2016: "Use of Mobile Technology for Information Collection and Dissemination": A DACS Technology Assessment Report: The Data & Analysis Center for Software (DACS) was one of several United States Department of Defense (DoD) sponsored Information Analysis Centers (IACs), administered by the Defense Technical Information Center (DTIC). It was managed by the U.S. Air Force Research Laboratory (AFRL) and operated by Quanterion Solutions Inc. under a long term DoD contract. The website is no longer available and was replaced by https://www.csiac.org/ DACS Report Number 518055:

Contract FA1500-10-D-0010; Prepared for the Defense Technical Information Center; Prepared By: Chet Hosmer, Chief Scientist; Carlton Jeffcoat, Vice President, Cyber Security Division; Matt Davis, Malware Analyst; Wetstone/Allen Corporation of America; 10400 Eaton Place; Fairfax, VA 22030; Thomas McGibbon, DACS Director; Quanterion Solutions Inc. 100 Seymour Road Utica, NY 13502. (Paragraphs 79-84 below were taken from the Report)

21. Mobile technology is increasingly being utilized as a tool for information dissemination and collection across the Government. The Department of Defense (DoD), Department of Homeland Security (DHS), Intelligence communities, and law enforcement are among those agencies utilizing mobile technology for information management. The primary mobile devices being utilized are the iPad®, iPhone®, Android™, and Windows Mobile™. The open architecture of these devices is advantageous for rapid application development and release.

22. New mobile technologies such as the iPhone®, iPad®, Android™ and similar devices have revolutionized the way information can be distributed. In the past, mobile devices such as Personal Data Assistants (PDAs) primarily focused on data storage and display. Today, an increasingly large number of devices are focusing not only on data storage and display, but also on communication and processing. As a result organizations have begun leveraging mobile technology as a means of information dissemination. These organizations include, but are not limited to, Government organizations such as the Department of Defense (DoD), the United States Army, the Department of Homeland Security (DHS), and a number of critical infrastructure organizations.

23. Significant advancements in mobile technology have occurred since September 11, 2001, both in the advancement of the devices and the infrastructures that support them. For example, mobile devices like the Android™ and iPad® can now operate equally and seamlessly via traditional cellular networks, as well as with infrastructure/ad hoc wireless networks.

24. The Defense Advanced Research Projects Agency (DARPA) has launched a program known as the Transformative Apps Program. The purpose of this program is to place the correct mobile applications into the hands of warfighters. To facilitate this, a military application store is being created to promote collaboration between developers and users in the field.

25. Another DoD initiative is Connecting Soldiers to Digital Applications (CSDA), sponsored by the Army Capabilities Integration Center (ARCIC) and the Army CIO/G6, with support from the Army Training and Doctrine Command (TRADOC) deputy commanding general for Initial Military Training, and other Army organizations. The purpose of this initiative is to determine the value of giving soldiers applications on mobile devices [ARMY]. During Phase One of the initiative the Army experimented with several types of smart phones to evaluate the effectiveness and usefulness of various mobile applications in the field. Devices tested included the Apple iPhone®, Google Android™ devices, and Microsoft Windows Mobile™ phones [C4ISR]. On these devices, applications were tested which covered a wide range of functions.

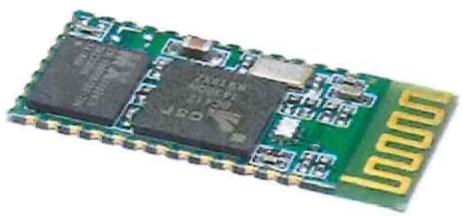
26. DoD is also starting to integrate chemical and biological sensors into mobile devices. Researchers from the University of California, San Diego have developed a miniature chemical sensor which can detect harmful gas in the air and

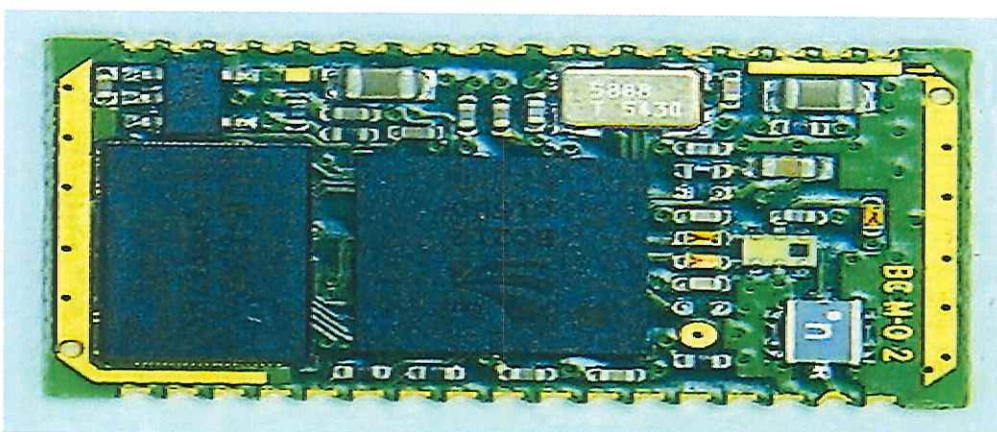
automatically send the information about the type and transmitting range of the gas. The chemical sensor is a silicon chip with hundreds of independent miniature sensors. These can identify the molecule of specific toxic gas and then report on it.

EXHIBIT 7

Claim Charts for the DHS; S&T "*Cell-All*" Initiative: Included is Synkera's MikroKera Ultra

Synkera presented the MikroKera Ultra Module at the Department of Homeland Security S&T "Cell-All" demonstration in Los Angeles on September 28, 2011. The aim of the project is to develop sensors that can detect life-threatening gases to be incorporated into cellphones as a crowd-sourced monitoring device. The success of the Synkera Bluetooth module and its fit into the Cell-All project headed by the Department of Homeland Security has been featured on numerous local and national news sites.





SYNKERA TECHNOLOGIES, INC.

Sensors
Membranes
Nanocomposites
Microcomponents

Security and Defense

Synkera specializes in solid-state sensors that feature excellent performance and reliability, all in a small form factor to enable simple chemical analysis. A key advantage of our technology is the ability to detect a wide range of dangerous chemicals including:

- Explosives
- Toxic Industrial Chemicals (TIC)
- Chemical Warfare Agents (CWA)
- Nerve Agents

Synkera's sensor technology enables better protection of warfighters and key infrastructure, providing the ability to produce situational awareness and actionable intelligence in real-time, via tracking of dangerous levels of hazardous chemicals that are very accessible to asymmetric threats.

Our **ProKera™** product line is an excellent choice for fixed monitoring applications, while our newest **MikroKera™** product line is pushing the boundaries on miniaturization and power consumption to enable distributed wireless sensor networks. The United States Department of Defense (DoD) and Department of Homeland Security (DHS) have repeatedly awarded grants to develop Synkera's sensor technology, and products are now being commercialized to meet the critical needs of these organizations.

2605 Trade Centre Avenue. Suite C. Longmont, CO 80503
(720) 494-8401

DHS S&T, California First Responders, Demonstrate Smart Phone-Based Chem Sensors

The Department of Homeland Security (DHS) and several agencies in California have demonstrated second-generation prototype chemical sensors that work with smart phones to detect the presence of toxic chemical compounds and provide alerts to first responders and emergency authorities to improve situational awareness of potentially hazardous events and terrorist attacks, thus enabling smarter decisions and faster response times.

The recent demonstration and training exercise included the DHS Science and Technology branch, the Los Angeles Fire and Police Departments and the California Environmental Protection Agency, as part of a response to a carbon monoxide leak in a hotel room. The demonstration of the Cell-All technology included two sensor prototypes, one developed by NASA's Ames Research Center and the other by the small firm Synkera Technologies and wireless technology company Qualcomm [QCOM].

The ultimate goal of Cell-All is the development of very low cost and very low power sensors that can be integrated directly into commercial smart phones such as a Blackberry, iPhone or Droid, that are in use by hundreds of millions of people. Such a vast deployment of sensors, which could be heavily concentrated in areas given the common use of smart phones, could enable the creation of a sensor network that warns of hazardous chemical events…
The sensor developed by Synkera and Qualcomm is about palm-size and also continuously sends real-time data to a smart phone while it is detecting an event.
https://www.defensedaily.com/dhs-st-california-first-responders-demonstrate-smart-phone-based-chem-sensors-2/uncategorized/

DHS; S&T Directorate; "Cell-All" Request: Adding the 1st Ind. claim of the 1st Patent ('497) issued to the Plaintiff (filed 04-05-06), illustrates infringement of Plaintiff's claimed invention the same as: Ind. claim 10 of the ('752) Patent; Ind. claim 1 of the ('189) Patent; Ind. claim 23 of the ('439) Patent; and, Ind. claim 5 of the ('287) Patent. An example of the infringement is demonstrated below in a claim chart using the specifications of LG Electronics (i.e. LG is representative of the specifications of Apple and Samsung) for the development, manufacture, and commercialization of a Cell-All "WMD Electronic Detection Device". The *Synkera "MikroKera Ultra"* integration with the CMDC Detection Device is also added.

LG Electronics: Electronic Detection Device	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1	Patent #: 8,106,752; Independent Claim 10	Patent #: 7,385,497; Independent Claim 1
DHS; S&T "Cell-All" initiative. Develop detection device to detect deadly chemicals". Stephen Dennis; PM: Contracts to Qualcomm, LG, Apple, and Samsung. Sensors will integrate with 261 million electronic devices (i.e. cell phones)	A monitoring device, comprising:	A cell phone comprising: *Note: This claim 23 of the '439 patent covers the 'new and improved' cell phone (utility patent requirement) the DHS requested in its Cell-All solicitation*	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:	A multi-sensor detection and lock disabling system for monitoring products and for detecting explosive, nuclear, contraband, chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:	A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:
The performance of LG's electronic detection devices: CPU that's at the core of the chipset is vital for the daily user experience and the general computing performance of the electronic detection devices (i.e. smartphone).	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;	at least one cell phone detector case having a front side, a rear side, a power source, and a Central processing unit (cpu);	a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);

LG electronic detection devices has an internal temperature sensor which monitors the CPU and battery temperature of device	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X	X	X
LG electronic detection devices, starting with LG G2, you can calibrate the motion sensor by going to Settings > General tab > Motion.	at least one motion sensor in communication with the at least one CPU;	X	X	X	X
LG's electronic detection devices: Thin Q has "the brightest" screen of any smartphone, thanks to its Super Bright Display technology.	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X	each detector case including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;	each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor
LG's electronic detection devices: GPS with A-GPS, GLONASS, and BDS	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;

LG's electronic detection devices: Wi-Fi, Wi-Fi Direct	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of… WiFi connection, internet connection, radio frequency (RF) connection, cellular connection… capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group… of satellite, Bluetooth, WiFi…	X	X
LG's electronic detection devices: cellular connection; Bluetooth	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a… Bluetooth connection, WiFi connection, internet connection… cellular connection… short range radio frequency (RF) connection, or GPS connection;	X	X	X
After multiple unsuccessful attempts, the LG electronic detection will automatically perform a factory data reset and all of the personal files will be erased.	at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;	whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;	X	an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained, and unequipped individuals; and	an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and

Battery Charging Specification, is power drawn from a USB port for charging. Three different sources of power: Standard downstream port (SDP), charging downstream port (CDP), and dedicated charging port (DCP). Wireless charging	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;
LG's electronic detection device features include sensors for face/smile detection, iris scanner, and fingerprint recognition.	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use	X	X

Cell-All: A wireless, wearable, mobile, device detects and identify chemicals in the air and sends detection data to another phone or a computer LG Watch Sport Smartwatch wireless, wearable, mobile, electronic detection device for chem / bio / human heart rate detection and monitoring at rest or active	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween…	a plurality of interchangeable cell phone sensors for detecting the chemical, biological, and radiological agents and compounds and capable of being disposed within the detector case;	a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;
Cell-All: The device detects and identify chemicals in the air and sends detection data to another phone (e.g. LG Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;	wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;	a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of at least one specific chemical, biological and radiological agent or compound;	a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;

The LG electronic detection device, NFC is a short-range high frequency wireless communication technology; enables the exchange of data between devices; share content between digital devices.	at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU…	X	X	X	X
Voice Mate (i.e. Quick Voice; Q Voice) built-in application for various LG electronic detection devices (i.e. smartphone); automatic activation features; when car engine is started; lock and unlock doors, activate and deactivate security systems. LG SmartThinQ® app for smart home appliances built on an open platform, so it will work with evolving smart technologies and devices for years to come. ***Cell-All***: The device detects and identify chemicals; sends to another phone	at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or… detect at least one of a chemical biological… agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device; a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;	whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and sends out a signal to another cell phone case, a handheld, a computer terminal located at a monitoring site, followed by and communicating with the cpu of the multi-sensor detection and automatic/mechanical lock disabler for exchanging information.	whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.

Voice Mate (i.e. Quick Voice; Q Voice) built-in application for various LG electronic detection devices (i.e. smartphone); automatic activation features; when car engine is started; lock and unlock doors, activate and deactivate security systems. LG SmartThinQ® app for smart home appliances built on an open platform, so it will work with evolving smart technologies and devices…	X	X	whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems	X	X
LG's electronic detection devices (i.e. at least LG G5 & LG V10 smartphones, and LG Watch Sport Smartwatch	X	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection… short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;	X	X

Cell-All: The device detects and identify chemicals in the air and sends detection data to another phone (e.g. LG Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	X	whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.	X	X	X

DHS; S&T Directorate; "Cell-All" Request: Adding the 1st Ind. claim of the 1st Patent ('497) issued to the Plaintiff (filed 04-05-06), illustrates infringement of Plaintiff's claimed invention the same as: Ind. claim 10 of the ('752) Patent; Ind. claim 1 of the ('189) Patent; Ind. claim 23 of the ('439) Patent; and, Ind. claim 5 of the ('287) Patent. An example of the infringement is demonstrated below in a claim chart using the specifications of Apple Inc. (i.e. Apple is representative of the specifications of LG and Samsung) for the development, manufacture, and commercialization of a Cell-All "WMD Electronic Detection Device". The *Synkera "MikroKera Ultra"* integration with the CMDC Detection Device is also added.

Apple Inc.: Electronic Detection Device	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1	Patent #: 8,106,752; Independent Claim 10	Patent #: 7,385,497; Independent Claim 1
DHS; S&T "Cell-All" initiative. Develop detection device to detect deadly chemicals". Stephen Dennis; PM: Contracts to Qualcomm, LG, Apple, and Samsung. Sensors will integrate with 261 million electronic devices (i.e. cell phones)	A monitoring device, comprising:	A cell phone comprising: *Note: This claim 23 of the '439 patent covers the 'new and improved' cell phone (utility patent requirement) the DHS requested in its Cell-All solicitation*	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:	A multi-sensor detection and lock disabling system for monitoring products and for detecting explosive, nuclear, contraband, chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:	A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:
The performance of Apple's electronic detection devices: CPU that's a part of the chipset is vital for the daily user experience and the general computing performance of the electronic detection devices (i.e. smartphone).	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front end processor for communication between a host computer and other devices;	at least one cell phone detector case having a front side, a rear side, a power source, and a Central processing unit (cpu);	a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);

Apple Files Patent for a new Temperature Sensor tied to a new Interactive Battery Indicator	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X	X	X
Apple's electronic detection devices: Apple M-series coprocessors are motion coprocessors used by Apple Inc. in their mobile devices.	at least one motion sensor in communication with the at least one CPU;	X	X	X	X
Apple's electronic detection devices: Highest color accuracy; full screen brightness & contrast; contrast ratio; lowest screen reflectance; smallest brightness variation	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X	each detector case including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;	each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor
Apple's electronic detection device: GPS with A-GPS, GLONASS	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;

Apple's electronic detection device: Wi-Fi, dual-band, hotspot	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of… WiFi connection, internet connection, radio frequency (RF) connection, cellular connection… capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group… of satellite, Bluetooth, WiFi…	X	X
Apple's electronic detection device: cellular connection; Bluetooth	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a… Bluetooth connection, WiFi connection, internet connection… cellular connection… short range radio frequency (RF) connection, or GPS connection;	X	X	X
Apple's electronic detection device includes a feature on that disables and erases all of the devices data after 10 failed passcode attempts.	at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;	whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;	X	an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained, and unequipped individuals; and	an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and

Apple's electronic detection device batteries and wall chargers which employ USB PD have the ability to charge devices up to 100W output using a USB-C connector	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;
Apple's electronic detection device features include sensors for face/smile detection, and fingerprint recognition.	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use	X	X

Cell-All: A wireless, wearable, mobile, device detects and identify chemicals in the air and sends detection data to another phone or a computer Apple Watch Series 3 electronic detection device for chem / bio / human heart rate detection and monitoring at rest or active	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween…	a plurality of interchangeable cell phone sensors for detecting the chemical, biological, and radiological agents and compounds and capable of being disposed within the detector case;	a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;
Cell-All: The device detects and identify chemicals in the air and sends detection data to another phone (e.g. Apple iPhone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center. WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;	wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;	a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of at least one specific chemical, biological and radiological agent or compound;	a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;

The Apple electronic detection device, NFC is a short-range high frequency wireless communication technology; enables the exchange of data between devices; share content between digital devices.	at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU…	X	X	X	X
Apple's Viper SmartStart: Start, locate and control your car with your iPhone, or Apple Watch. "Nice": Manages the gate and garage door from your iPhone or Apple Watch using the Home app (i.e. voice) Siri. Apple HomeKit is a system that controls smart home devices. Viper system in your car so you can start, lock and unlock your car ***Cell-All***: The device detects and identify chemicals in the air sends detection data to another phone	at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or… detect at least one of a chemical biological… agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device; a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;	whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and sends out a signal to another cell phone case, a handheld, a computer terminal located at a monitoring site, followed by and communicating with the cpu of the multi-sensor detection and automatic/mechanical lock disabler for exchanging information.	whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.

Apple's Viper SmartStart: Start, locate and control your car with your iPhone, or Apple Watch. "Nice": Manages the gate and garage door from your iPhone or Apple Watch using the Home app (i.e. voice) Siri. Apple HomeKit is a system that controls smart home devices. Viper system in your car so you can start, lock and unlock your car	X	X	whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems	X	X
Apple electronic detection devices (i.e. at least iPhone 7 & iPhone 8 smartphones, and Apple Watch Series 3	X	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection… short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;	X	X

Cell-All: The device detects and identify chemicals in the air and sends detection data to another phone (e.g. Apple Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	X	whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.	X	X	X

DHS; S&T Directorate; "Cell-All" Request: Adding the 1st Ind. claim of the 1st Patent ('497) issued to the Plaintiff (filed 04-05-06), illustrates infringement of Plaintiff's claimed invention the same as: Ind. claim 10 of the ('752) Patent; Ind. claim 1 of the ('189) Patent; Ind. claim 23 of the ('439) Patent; and, Ind. claim 5 of the ('287) Patent. An example of the infringement is demonstrated below in a claim chart using the specifications of Samsung Electronics (i.e. Samsung is representative of the specifications of LG and Apple) for the development, manufacture, and commercialization of a Cell-All "WMD Electronic Detection Device". The *Synkera "MikroKera Ultra"* integration with the CMDC Detection Device is also added.

Samsung: Electronic Detection Device	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1	Patent #: 8,106,752; Independent Claim 10	Patent #: 7,385,497; Independent Claim 1
DHS; S&T "Cell-All" initiative. Develop detection device to detect deadly chemicals". Stephen Dennis; PM: Contracts to Qualcomm, LG, Apple, and Samsung. Sensors will integrate with 261 million electronic devices (i.e. cell phones)	A monitoring device, comprising:	A cell phone comprising: *Note: This claim 23 of the '439 patent covers the 'new and improved' cell phone (utility patent requirement) the DHS requested in its Cell-All solicitation*	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:	A multi-sensor detection and lock disabling system for monitoring products and for detecting explosive, nuclear, contraband, chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:	A multi sensor detection and lock disabling system for monitoring products and for detecting chemical, biological, and radiological agents and compounds so that terrorist activity can be prevented, comprising:
The performance of Samsung's electronic detection devices: CPU that's a part of the chipset is vital for the daily user experience and the general computing performance of the electronic detection devices (i.e. smartphone).	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;	at least one cell phone detector case having a front side, a rear side, a power source, and a Central processing unit (cpu);	a detector case including a front side, a rear side, a power source and a Central Processing Unit (cpu);

Samsung's electronic detection devices has various sensors like the temperature sensor for the battery and the CPU or processor.	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X	X	X
Samsung's electronic detection devices accelerometers handle axis-based motion sensing—reason why the smartphone can track steps without a separate wearable.	at least one motion sensor in communication with the at least one CPU;	X	X	X	X
Samsung's electronic detection device has set the bar with the highest-rated smartphone displays. With a panel produced by Samsung, and optimized by Apple	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X	each detector case including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor;	each detector including a sound alarm indicator, a readings panel, a light alarm indicator and a sensor
Samsung's electronic detection device: GPS with A-GPS, GLONASS, BDS, GALILEO	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;

Samsung's electronic detection device: Wi-Fi, dual-band, Wi-Fi Direct, hotspot	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of… WiFi connection, internet connection, radio frequency (RF) connection, cellular connection… capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the… device and transceivers of the products is a type or types selected from the group… of satellite, Bluetooth, WiFi…	X	X
Samsung's electronic detection device: cellular connection; Bluetooth	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a… Bluetooth connection, WiFi connection, internet connection… cellular connection… short range radio frequency (RF) connection, or GPS connection;	X	X	X
Samsung's electronic detection device: After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung device automatically locks itself up. If unable to log in after the security layers, the only option is to have the device unlocked.	at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;	whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;	X	an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained, and unequipped individuals; and	an automatic/mechanical lock disabler interconnected to the cpu and which is mounted to a lock on a product for receiving transmission from the cpu to lock or disable the lock on the product to prevent access to the product by unauthorized, untrained and unequipped individuals; and

Samsung's electronic detection devices Fast Charge power bank has a capacity of 5,100mAh and can provide up to 1.5 charges for the majority of smartphones. The power bank has an LED power indicator; comes with a micro USB cable and a micro USB to USB Type-C adapter.	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;	an Internet connection, a GPS connection, and a power connection located on the rear side and which are interconnected with the cpu;
Samsung's electronic detection devices allows fingerprints to set-up the fingerprint scanner for easy log-in and lock-out. Face unlock uses the front-facing camera to identify the user and unlock the device. Iris scanning uses special sensors on front of phone to identify and unlock the device.	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop… is locked by the biometric lock disabler to prevent unauthorized use	X	X

Cell-All: wireless, wearable, mobile, device detects and identify chemicals in the air using a "sample jet" and sends detection data to another phone or a computer Samsung S3 Classic electronic detection device for chem / bio / human heart rate detection and monitoring at rest or active	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween…	a plurality of interchangeable cell phone sensors for detecting the chemical, biological, and radiological agents and compounds and capable of being disposed within the detector case;	a plurality of interchangeable detectors for detecting the chemical, biological and radiological agents and compounds and capable of being disposed within the detector case;
Cell-All: The device detects and identify chemicals in the air using a "sample jet" and sends detection data to another phone (e.g. Samsung Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center. WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;	at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;	wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;	a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of at least one specific chemical, biological and radiological agent or compound;	a plurality of indicator lights located on the front side with each indicator light corresponding to and indicating the detection of one specific chemical, biological and radiological agent and compound;

Samsung's electronic detection device, near-field communication (NFC) Ring can unlock the device. The NFC Ring has two NFC tag inlays inside the ring and can be used to unlock & control mobile devices	at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU…	X	X	X	X
The Samsung SmartThings contains: one SmartThings Hub, two SmartThings Multipurpose Sensors, one SmartThings Motion Sensor, and one SmartThings Outlet. Connects to appliances, lights, locks, cameras, thermostats, sensors. Get alerts on smartphone if motion in the home. BMW Digital Key to lock/unlock; and start it up with Samsung phones only. ***Cell-All:*** The device detects and identify chemicals in the air using a "sample jet" sends detection data to another phone	at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or… detect at least one of a chemical biological… agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device; a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;	whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and sends out a signal to another cell phone case, a handheld, a computer terminal located at a monitoring site, followed by and communicating with the cpu of the multi-sensor detection and automatic/mechanical lock disabler for exchanging information.	whereupon detection of specific chemical, biological, or radiological agents or compounds by the detectors causes the lighting of the corresponding indicator light for visual confirmation of the detection and initiates signal transmission from the cpu to the automatic/mechanical lock disabler to lock or disable the lock of the product thereby preventing further contamination about the product and denying access to the product by unauthorized, untrained and unequipped individuals.

The Samsung SmartThings Home Monitoring Kit contains: one SmartThings Hub, two SmartThings Multipurpose Sensors, one SmartThings Motion Sensor, and one SmartThings Outlet. Connects to appliances, lights, speakers, locks, cameras, thermostats, sensors. Get alerts on smartphone if there's unexpected entry or motion in the home.	X	X	whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems	X	X
Samsung electronic detection devices (i.e. at least the Galaxy Note 8 & Galaxy S8 smartphones, and Samsung Gear S3 Classic	X	a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;	wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection… short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;	X	X

Cell-All: The device detects and identify chemicals in the air using a "sample jet" and sends detection data to another phone (e.g. Samsung Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center. WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	X	whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.	X	X	X

Government Third Party Contractors' CMDC Devices Manufactured "*for*" the Government in the DHS; S&T "*Cell-All*" initiative

LG Electronics: CMDC Device	**Apple Inc.: CMDC Device**	**Samsung: CMDC Device**
DHS; S&T "Cell-All" initiative. Develop detection device to detect deadly chemicals". Stephen Dennis; PM: Contracts to LG, Apple, and Samsung. Sensors will integrate with 261 million CMDC devices (i.e. cell phones)	DHS; S&T "Cell-All" initiative. Develop detection device to detect deadly chemicals". Stephen Dennis; PM: Contracts to LG, Apple, and Samsung. Sensors will integrate with 261 million CMDC devices (i.e. cell phones)	DHS; S&T "Cell-All" initiative. Develop detection device to detect deadly chemicals". Stephen Dennis; PM: Contracts to LG, Apple, and Samsung. Sensors will integrate with 261 million CMDC devices (i.e. cell phones)
The performance of LG's CMDC detection devices: CPU that's at the core of the chipset is vital for the daily user experience and the general computing performance of the CMDC detection devices (i.e. smartphone).	The performance of Apple's CMDC detection devices: CPU that's a part of the chipset is vital for the daily user experience and the general computing performance of the CMDC detection devices (i.e. smartphone).	The performance of Samsung's CMDC detection devices: CPU that's a part of the chipset is vital for the daily user experience and the general computing performance of the CMDC detection devices (i.e. smartphone).
LG CMDC detection devices has an internal temperature sensor which monitors the CPU and battery temperature of device	Apple Files Patent for a new Temperature Sensor tied to a new Interactive Battery Indicator	Samsung's CMDC detection devices has various sensors like the temperature sensor for the battery and the CPU or processor.
LG CMDC detection devices, starting with LG G2, you can calibrate the motion sensor by going to Settings > General tab > Motion.	Apple's CMDC detection devices: Apple M-series coprocessors are motion coprocessors used by Apple Inc. in their CMDC devices.	Samsung's CMDC detection devices accelerometers handle axis-based motion sensing—reason why the smartphone can track steps without a separate wearable.

LG's CMDC detection devices: Thin Q has "the brightest" screen of any smartphone, thanks to its Super Bright Display technology.	Apple's CMDC detection devices: Highest absolute color accuracy; full screen brightness; full screen contrast; contrast ratio; lowest screen reflectance; smallest brightness variation	Samsung's CMDC detection device has set the bar with the highest-rated smartphone displays. With a panel produced by Samsung, and optimized by Apple
LG's CMDC detection devices: GPS with A-GPS, GLONASS, and BDS	Apple's CMDC detection device: GPS with A-GPS, GLONASS	Samsung's CMDC detection device: GPS with A-GPS, GLONASS, BDS, GALILEO
LG's CMDC detection devices: Wi-Fi, Wi-Fi Direct	Apple's CMDC detection device: Wi-Fi, dual-band, hotspot	Samsung's CMDC detection device: Wi-Fi, dual-band, Wi-Fi Direct, hotspot
LG's CMDC detection devices: cellular connection; Bluetooth	Apple's CMDC detection device: cellular connection; Bluetooth	Samsung's CMDC detection device: cellular connection; Bluetooth

LG's CMDC detection device. After multiple unsuccessful attempts, the LG CMDC detection device will automatically perform a factory data reset and all of the personal files will be erased.	Apple's CMDC detection device includes a feature on that disables and erases all of the CMDC devices' data after 10 failed passcode attempts.	Samsung's CMDC detection device: After several unsuccessful log-in attempts using a passcode or fingerprint, a Samsung CMDC device automatically locks itself up. If unable to log in after the security layers, the only option is to have the device unlocked.
LG's CMDC detection device. Battery Charging Specification, is power drawn from a USB port for charging. Three different sources of power: Standard downstream port (SDP), charging downstream port (CDP), and dedicated charging port (DCP). Wireless charging	Apple's CMDC detection device batteries and wall chargers which employ USB PD have the ability to charge the CMDC devices up to 100W output using a USB-C connector	Samsung's CMDC detection devices Fast Charge power bank has a capacity of 5,100mAh and can provide up to 1.5 charges for the majority of CMDC devices. The power bank has an LED power indicator; comes with a micro USB cable and a micro USB to USB Type-C adapter.
LG's CMDC detection device features include sensors for face/smile detection, iris scanner, and fingerprint recognition.	Apple's CMDC detection device features include sensors for face/smile detection, and fingerprint recognition.	Samsung's CMDC detection devices allows fingerprints to set-up the fingerprint scanner for easy log-in and lock-out. Face unlock uses the front-facing camera to identify the user and unlock the CMDC device. Iris scanning uses special sensors on front of phone to identify and unlock the CMDC device.

Cell-All: A wireless, wearable, mobile, device detects and identify chemicals in the air using a "sample jet" and sends detection data to another phone or a computer LG Watch Sport Smartwatch wireless, wearable, mobile CMDC detection device for chem / bio / human heart rate detection and monitoring at rest or active	***Cell-All:*** A wireless, wearable, mobile, device detects and identify chemicals in the air using a "sample jet" and sends detection data to another phone or a computer Apple Watch Series 3 wireless, wearable, mobile CMDC detection device for chem / bio / human heart rate detection and monitoring at rest or active	***Cell-All***: A wireless, wearable, mobile, device detects and identify chemicals in the air using a "sample jet" and sends detection data to another phone or a computer Samsung S3 Classic wireless, wearable, mobile CMDC detection device for chem / bio / human heart rate detection and monitoring at rest or active
Cell-All: The device detects and identify chemicals in the air and sends detection data to another CMDC device (e.g. LG Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	***Cell-All***: The device detects and identify chemicals in the air and sends detection data to another CMDC device (e.g. Apple Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center. WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	***Cell-All***: The device detects and identify chemicals in the air using a "sample jet" and sends detection data to another CMDC device (e.g. Samsung Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center. WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology
The LG CMDC detection device, NFC is a short-range high frequency wireless communication technology; enables the exchange of data between CMDC devices; share content between digital CMDC devices.	The Apple CMDC detection device, NFC is a short-range high frequency wireless communication technology; enables the exchange of data between CMDC devices; share content between digital CMDC devices.	Samsung's CMDC detection device, near-field communication (NFC) Ring can unlock the CMDC device. The NFC Ring has two NFC tag inlays inside the ring and can be used to unlock & control CMDC devices

LG's Voice Mate (i.e. Quick Voice; Q Voice) built-in application for various LG CMDC detection devices (i.e. smartphone); automatic activation features; when car engine is started; lock and unlock doors, activate and deactivate security systems. LG SmartThinQ® app for smart home appliances built on an open platform, so it will work with evolving smart technologies and CMDC devices for years to come. ***Cell-All***: The CMDC device detects and identify chemicals in the air using a "sample jet" sends detection data to another CMDC device	Apple's Viper SmartStart: Start, locate and control your car with your Apple CMDC phone or CMDC watch. "Nice": Manages the gate and garage door from your CMDC phone or CMDC watch using the Home app (i.e. voice) Siri. Apple HomeKit is a system that controls smart home devices. Viper system in your car so you can start, lock and unlock your car ***Cell-All***: The CMDC device detects and identify chemicals in the air using a "sample jet" sends detection data to another CMDC device	The Samsung SmartThings contains: one SmartThings Hub, two SmartThings Multipurpose Sensors, one SmartThings Motion Sensor, and one SmartThings Outlet. Connects to appliances, lights, locks, cameras, thermostats, sensors. Get alerts on CMDC phone or CMDC watch if motion in the home. BMW Digital Key to lock/unlock; and start it up with Samsung's CMDC devices only. ***Cell-All***: The CMDC device detects and identify chemicals in the air using a "sample jet" sends detection data to another CMDC device
LG's Voice Mate (i.e. Quick Voice; Q Voice) built-in application for various LG CMDC detection devices (i.e. smartphone); automatic activation features; when car engine is started; lock and unlock doors, activate and deactivate security systems. LG SmartThinQ® app for smart home appliances built on an open platform, so it will work with evolving smart technologies and devices…	Apple's Viper SmartStart: Start, locate and control your car with your CMDC Phone, or CMDC Apple Watch. "Nice": Manages the gate and garage door from your CMDC Phone or CMDC Apple Watch using the Home app (i.e. voice) Siri. Apple HomeKit is a system that controls smart home devices. Viper system in your car so you can start, lock and unlock your car	The Samsung SmartThings Home Monitoring Kit contains: one SmartThings Hub, two SmartThings Multipurpose Sensors, one SmartThings Motion Sensor, and one SmartThings Outlet. Connects to appliances, lights, speakers, locks, cameras, thermostats, sensors. Get alerts on CMDC smartphone if there's unexpected entry or motion in the home.

LG's CMDC detection devices (i.e. at least LG G5 & LG V10 smartphones, and LG Watch Sport Smartwatch)	Apple CMDC detection devices (i.e. at least iPhone 7, 8, 9 & 11 smartphones, and Apple Watch Series 3 & 4)	Samsung CMDC detection devices (i.e. at least the Galaxy Note 8 & Galaxy S8 smartphones, and Samsung Gear S3 Classic)
Cell-All: The CMDC device detects and identify chemicals in the air and sends detection data to another CMDC device (e.g. LG Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	***Cell-All:*** The CMDC device detects and identify chemicals in the air and sends detection data to another CMDC device (e.g. Apple Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology	***Cell-All***: The CMDC device detects and identify chemicals in the air using a "sample jet" and sends detection data to another CMDC device (e.g. Samsung Smartphone) or a computer "How does it work?" Shows indicator lights for the monitoring device; relayed over a cellular network to the monitoring center. WMD sensor development for the Cell-All Initiative: Qualcomm, NASA, and Rhevision Technology

Third Party Government Contractor (Apple Inc.) was Issued the *First* Patent for the CMDC Device

DESIGN CHART FOR APPLE'S CMDC DEVICE v. PLAINTIFF'S CMDC DEVICE

Apple's 1st Patent for the CMDC device (i.e. smartphone; electronic device) ornamental design: First application filing date is January 5, 2007 (App. No: 29/270,887). Patent No: D558756	**Plaintiff's 1st Patent for the CMDC device (i.e. detector Case; electronic device) ornamental design: USPTO Disclosure Document filed Nov. 17, 2004; First application filing date is April 5, 2006 (App. No: 11/397,118). Patent No: 7,385,497**
CMDC Device: "The device (i.e. electronic device) which controls the flow of electrons is called electronic device. These devices are the main building blocks of electronic circuits. The various electronic devices are computers, mobile phones, etc." Retrieved from: https://www.physics-and-radio-electronics.com/electronic-devices-and-circuits.html	CMDC Device: The detector case includes a power source (battery or electrical) … A cpu 40 is mounted within the detector case 12 and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates
FIG. 1 is a front perspective view of an electronic device in accordance with the present design.	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
FIG. 2 is a rear perspective view for the electronic device.	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
FIG. 3 is a front view for the electronic device.	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30

FIG. 4 is a rear view for the electronic device.	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
FIG. 5 is a top view for the electronic device.	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
FIG. 6 is a bottom view for the electronic device.	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
FIG. 7 is a left side view for the electronic device; and,	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
FIG. 8 is a right side view for the electronic device	The detector case 12 includes a top 22, a bottom 24, a pair of opposed sides 26 and a front side or panel 28 and an opposite rear or back side 30
The broken lines depicted in FIGS. 1, 2, and 6 of the inner rectangle, at the center bottom of the electronic device, represent the bounds of the claimed design, while the broken lines inside the rectangle, shown only in FIG. 6, are directed to environment and are for illustrative purposes only; the broken lines from no part of the claimed design.	Fig. 1 is an illustrative drawing of the rectangle design of the detector case; and, Fig. 17 are illustrative drawings of the rectangle design of the cell phone (i.e. smartphone) and the cell phone detector case

The article is not limited to the scale shown herein. As indicated in the title, the article of manufacture to which the ornamental design has been applied is an electronic device. Examples of an electronic device are a computer, a portable or hand-held device, a personal digital assistant, a communication device (e.g., cellular phone), a novelty item, toy, and/or the like.	FIG. 15 is a representative schematic view of… a monitoring PC or computer terminal. It is another objective of the present invention to provide… products grouped together by common features in several product groupings such as design similarity… product grouping strategy has been developed wherein products… having the same or similar design… [i]n addition to grouping products together by features, designs and materials… FIG. 17 is a perspective view... of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case
The first iPhone featured a two-tone back that was mostly made of aluminum — a design element that the company would return to this year with the release of the iPhone 5 with a predominantly metal back. Apple's interim devices opted for different materials: The iPhone 3G and 3GS had plastic backs, while the iPhone 4 and 4S backs were made of glass. Retrieved from: https://appleinsider.com/articles/12/12/18/apple-wins-patent-for-first-iphone-designed-by-jobs-ive	… [P]roduct grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design… [i]n addition to grouping products together by features, designs and materials… the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted)… the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include… mobile communication devices… personal computers (PCs), laptops, cell phones, personal digital assistants (PDAs)… handhelds

Third Party Government Contractors CMDC Designs

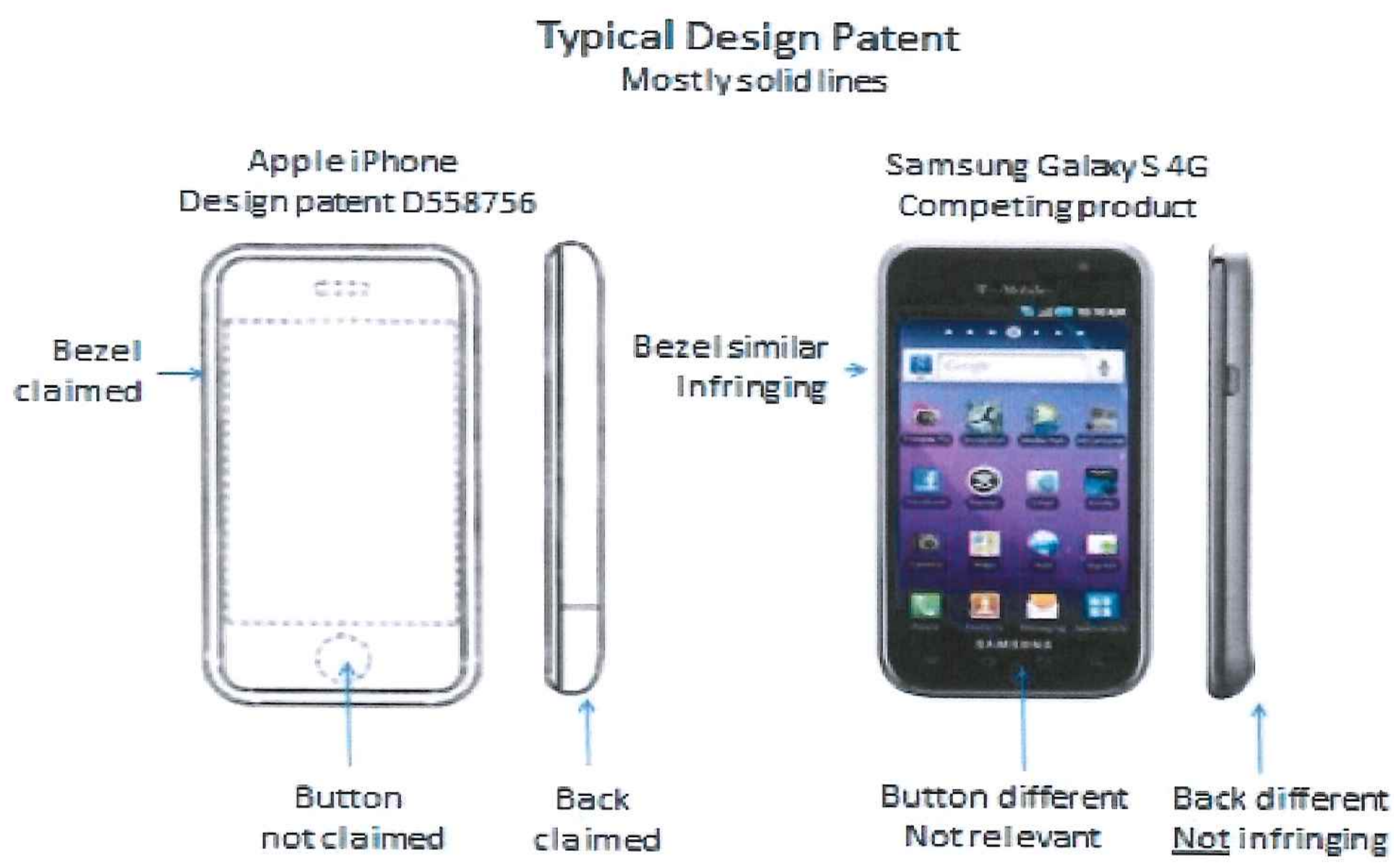
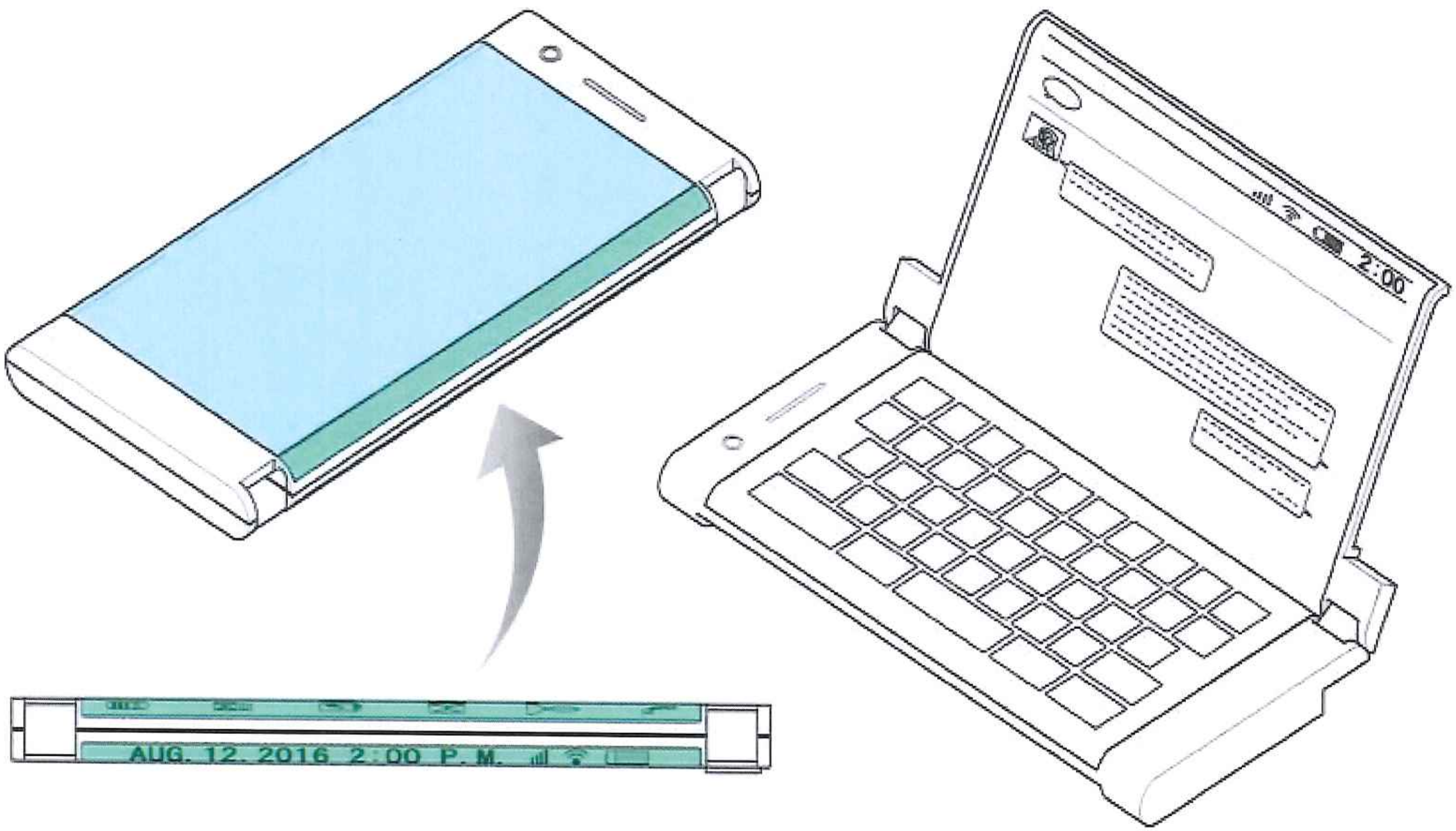
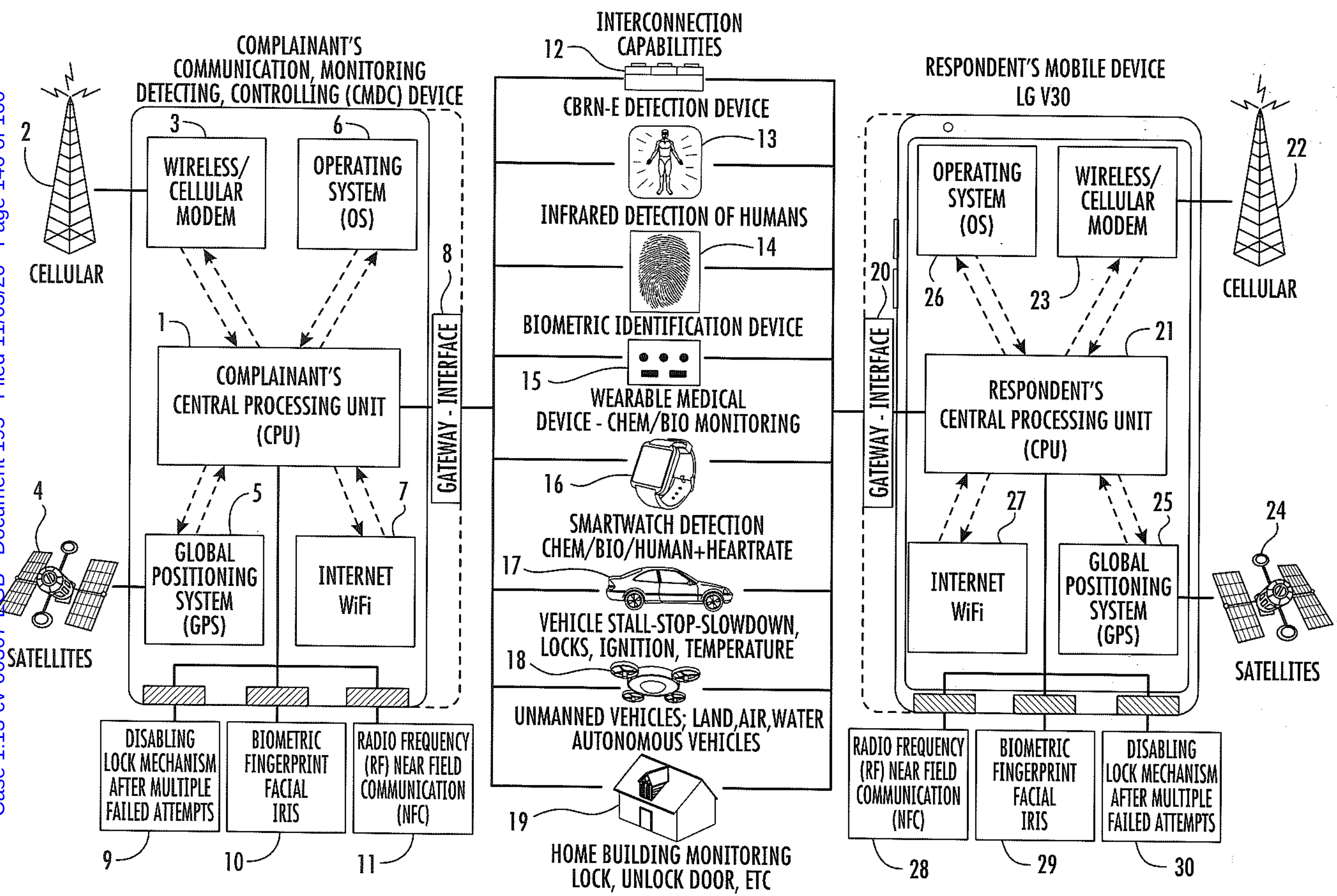


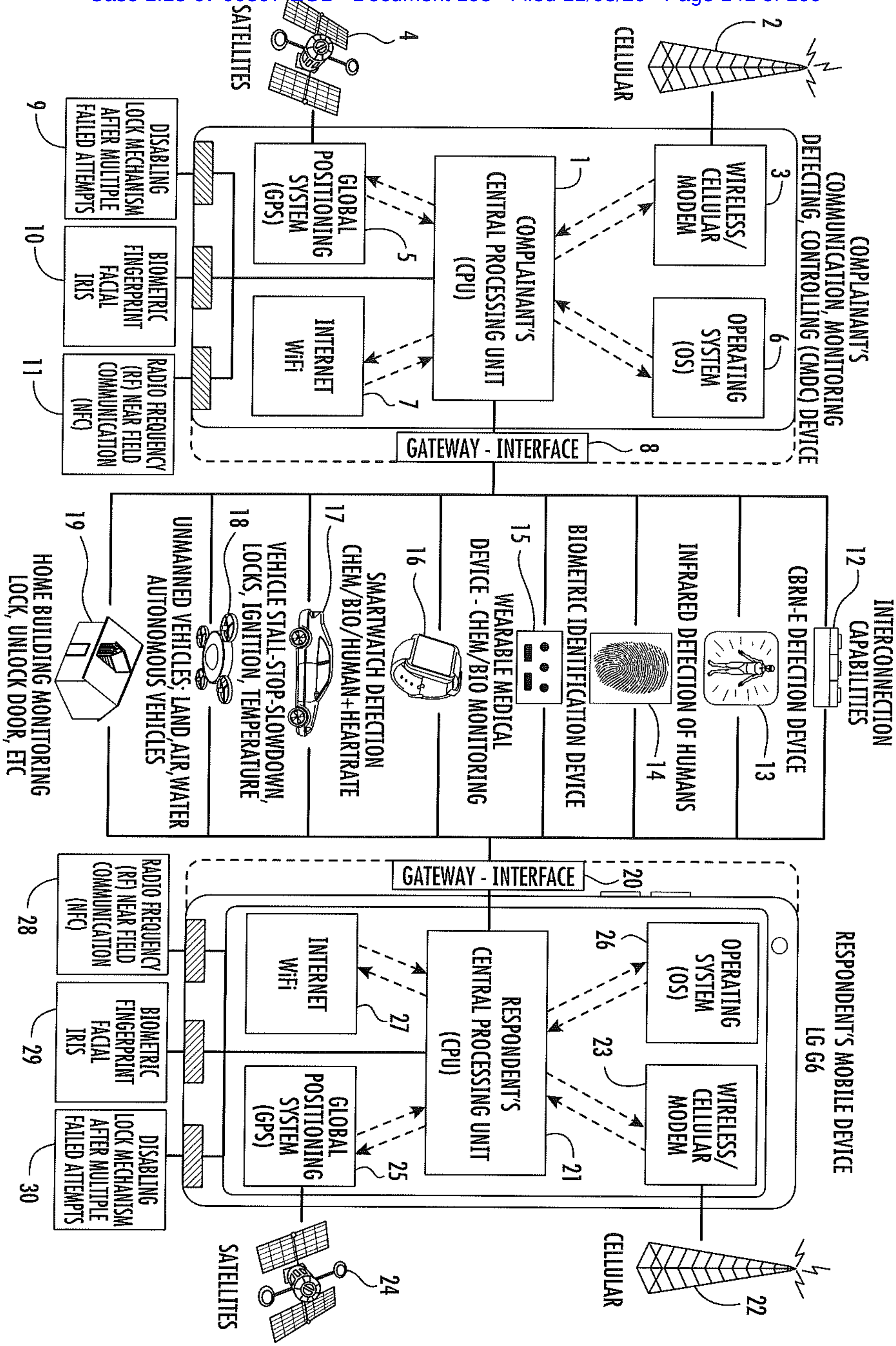
Figure 1

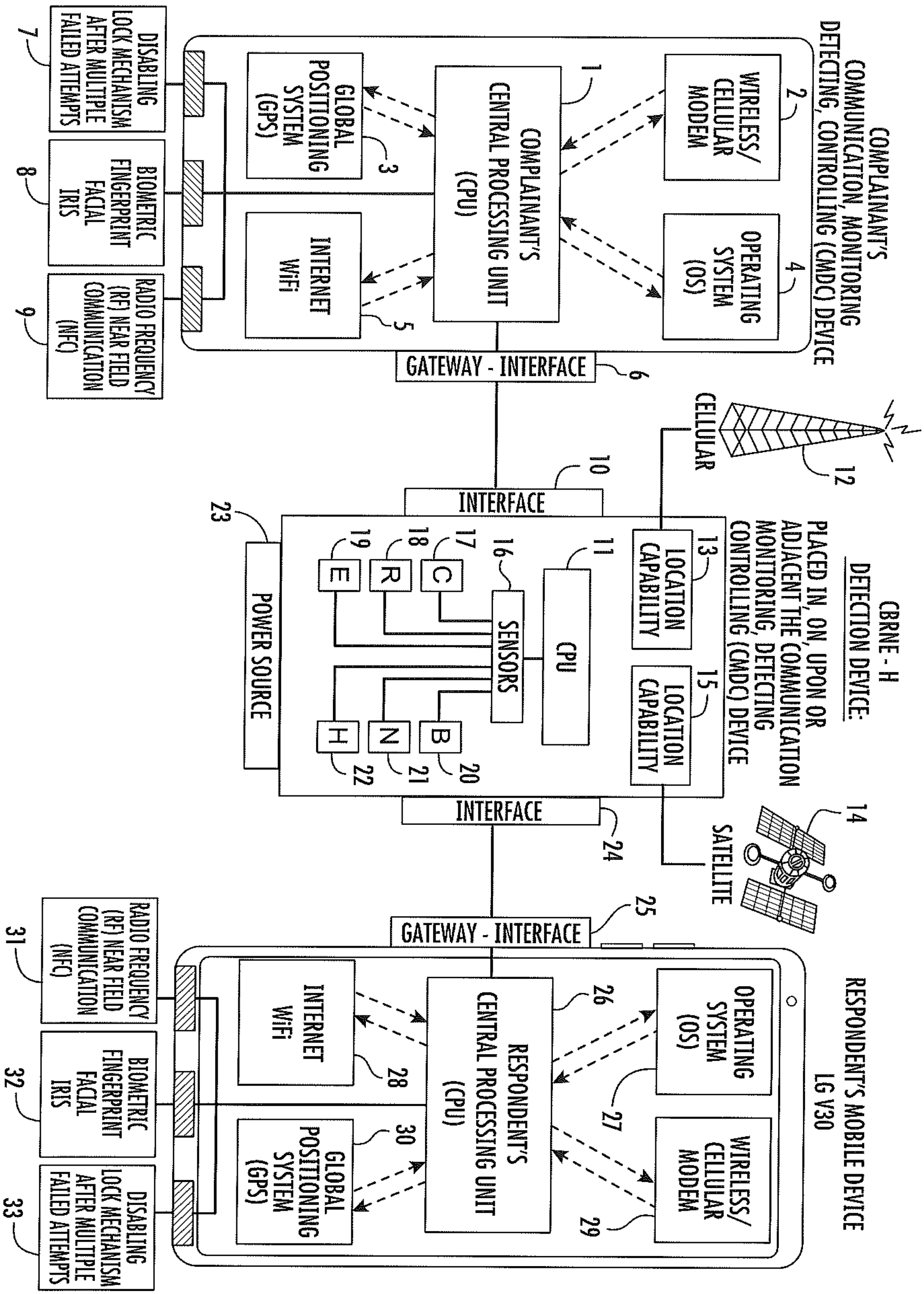
LG Electronics FOLDABLE SMARTPHONE WITH CURVED DISPLAY LETSGO DIGITAL



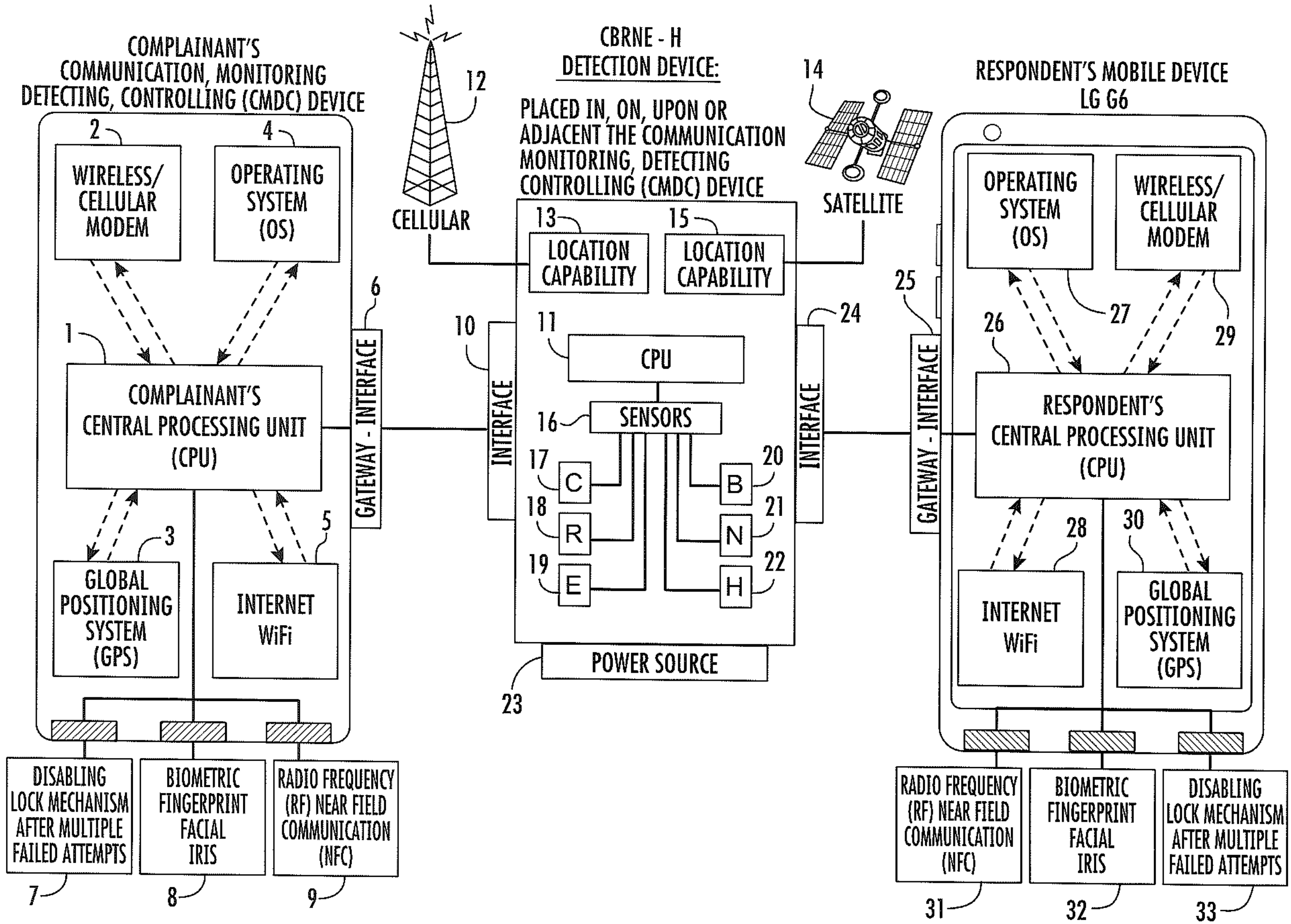
Third Party Government Contractor (LG Electronics) Utility Specifications and Capabilities for the CMDC Device

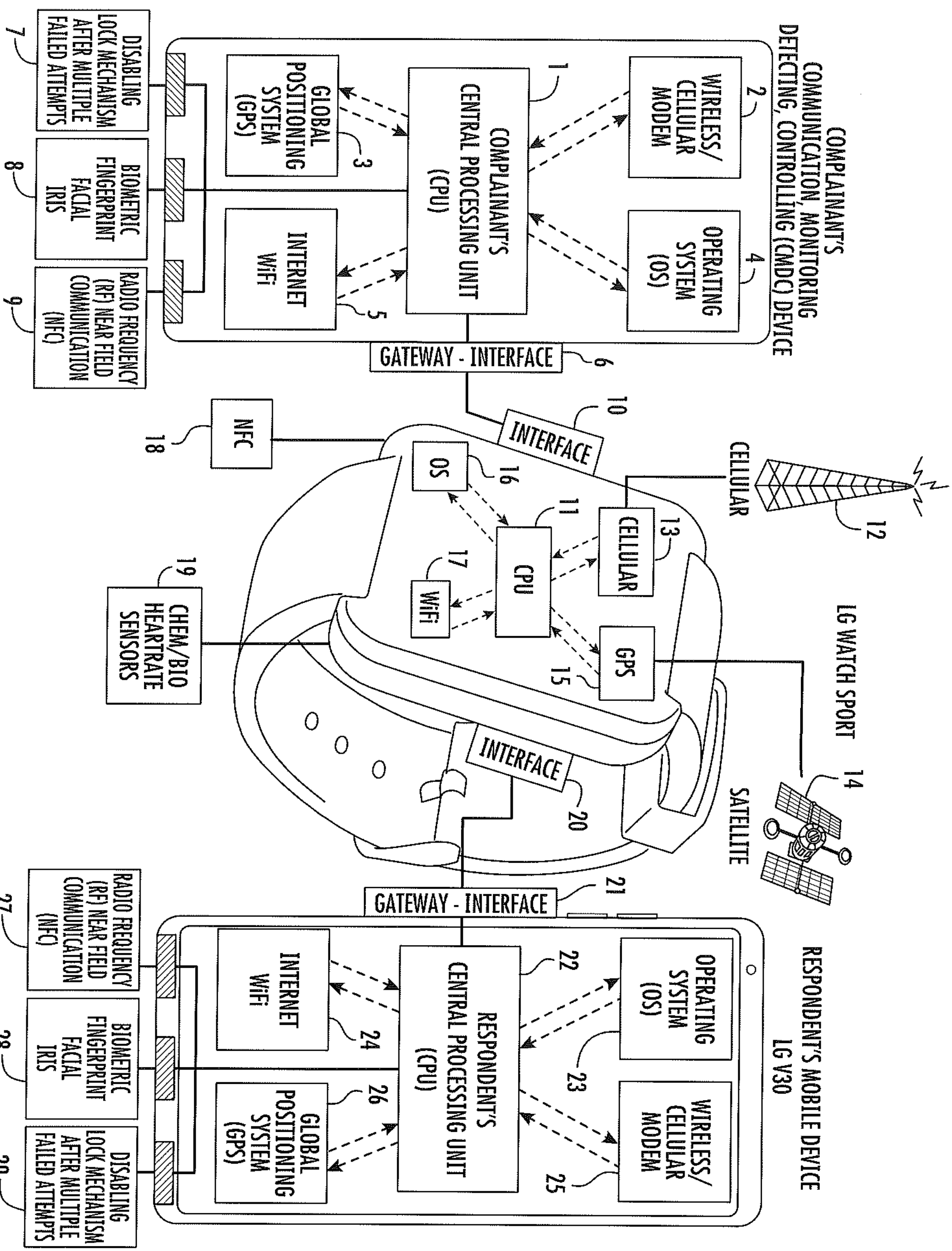

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
2
CELLULAR
3
WIRELESS/ CELLULAR MODEM
6
OPERATING SYSTEM (OS)
8
GATEWAY - INTERFACE
1
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
4
SATELLITES
5
GLOBAL POSITIONING SYSTEM (GPS)
7
INTERNET WiFi
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
9
BIOMETRIC FINGERPRINT FACIAL IRIS
10
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
11
INTERCONNECTION CAPABILITIES
12
CBRN-E DETECTION DEVICE
13
INFRARED DETECTION OF HUMANS
14
BIOMETRIC IDENTIFICATION DEVICE
15
WEARABLE MEDICAL DEVICE - CHEM/BIO MONITORING
16
SMARTWATCH DETECTION CHEM/BIO/HUMAN+HEARTRATE
17
VEHICLE STALL-STOP-SLOWDOWN, LOCKS, IGNITION, TEMPERATURE
18
UNMANNED VEHICLES; LAND,AIR,WATER AUTONOMOUS VEHICLES
19
HOME BUILDING MONITORING LOCK, UNLOCK DOOR, ETC
RESPONDENT'S MOBILE DEVICE LG V30
22
CELLULAR
20
GATEWAY - INTERFACE
OPERATING SYSTEM (OS)
26
WIRELESS/ CELLULAR MODEM
23
21
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
27
INTERNET WiFi
25
GLOBAL POSITIONING SYSTEM (GPS)
24
SATELLITES
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
28
BIOMETRIC FINGERPRINT FACIAL IRIS
29
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
30

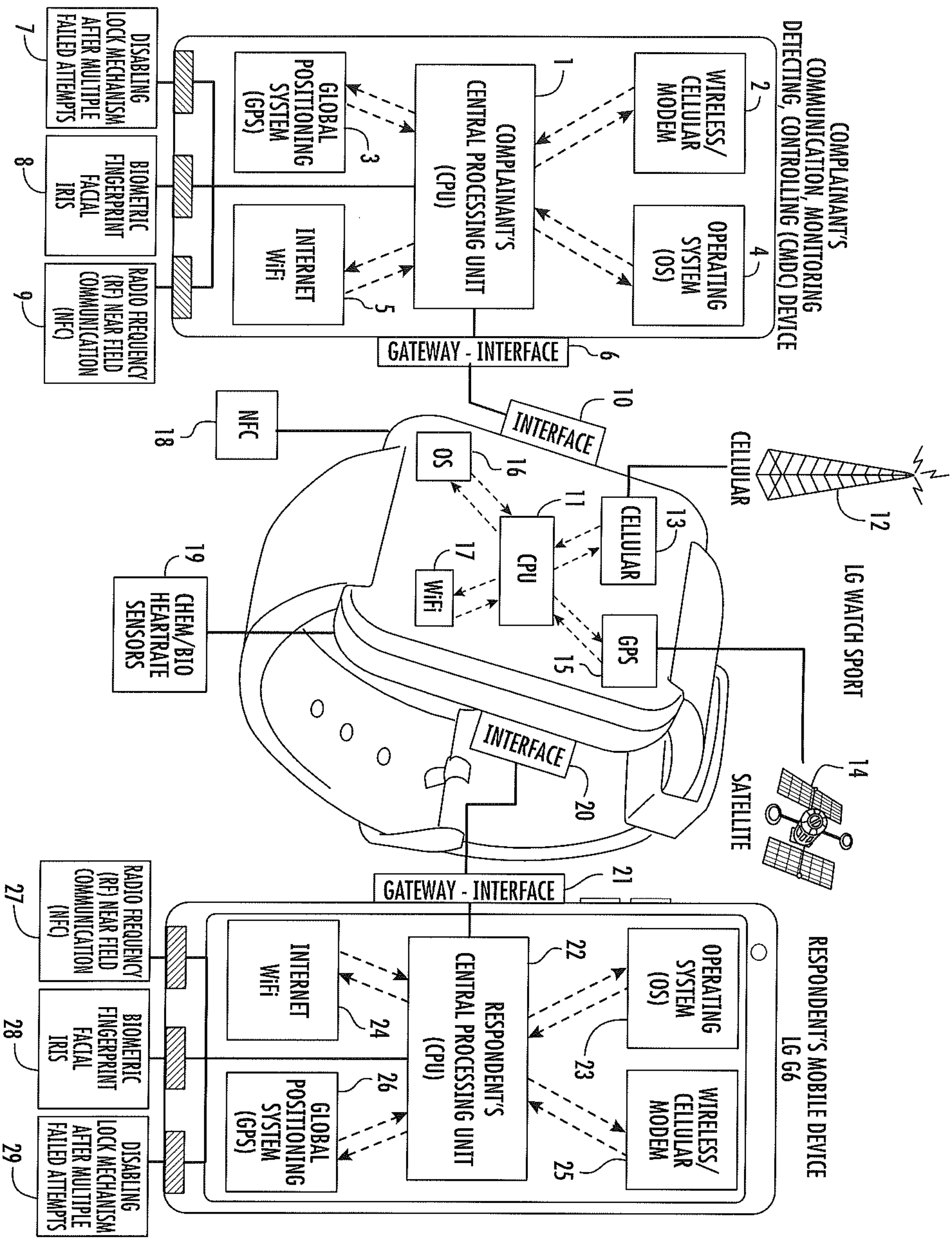

2
CELLULAR
4
SATELLITES
COMPLAINANT'S
COMMUNICATION, MONITORING
DETECTING, CONTROLLING (CMDC) DEVICE
3
WIRELESS/
CELLULAR
MODEM
6
OPERATING
SYSTEM
(OS)
1
COMPLAINANT'S
CENTRAL PROCESSING UNIT
(CPU)
5
GLOBAL
POSITIONING
SYSTEM
(GPS)
INTERNET
WiFi
7
GATEWAY - INTERFACE
8
9
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
10
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
11
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
12
INTERCONNECTION
CAPABILITIES
CBRN-E DETECTION DEVICE
13
INFRARED DETECTION OF HUMANS
14
BIOMETRIC IDENTIFICATION DEVICE
15
WEARABLE MEDICAL
DEVICE - CHEM/BIO MONITORING
16
SMARTWATCH DETECTION
CHEM/BIO/HUMAN+HEARTRATE
17
VEHICLE STALL-STOP-SLOWDOWN,
LOCKS, IGNITION, TEMPERATURE
18
UNMANNED VEHICLES: LAND,AIR,WATER
AUTONOMOUS VEHICLES
19
HOME BUILDING MONITORING
LOCK, UNLOCK DOOR, ETC
GATEWAY - INTERFACE
20
RESPONDENT'S MOBILE DEVICE
LG G6
26
OPERATING
SYSTEM
(OS)
23
WIRELESS/
CELLULAR
MODEM
RESPONDENT'S
CENTRAL PROCESSING UNIT
(CPU)
21
INTERNET
WiFi
27
GLOBAL
POSITIONING
SYSTEM
(GPS)
25
28
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
29
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
30
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
CELLULAR
22
SATELLITES
24



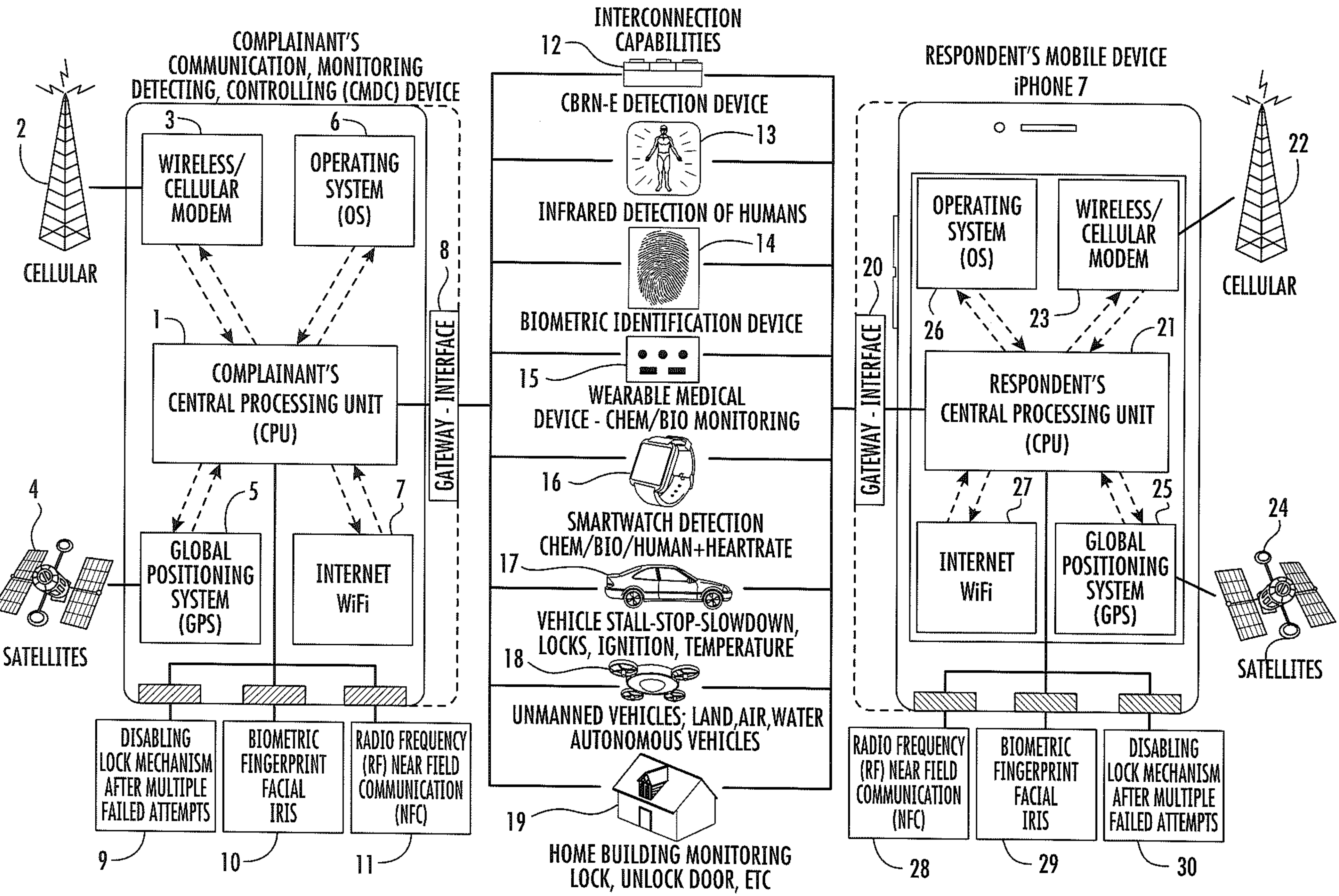
COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
1
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
GATEWAY - INTERFACE
6
CELLULAR
12
10
INTERFACE
CBRNE - H DETECTION DEVICE:
PLACED IN, ON, UPON OR ADJACENT THE COMMUNICATION MONITORING, DETECTING CONTROLLING (CMDC) DEVICE
13
LOCATION CAPABILITY
15
LOCATION CAPABILITY
11
CPU
16
SENSORS
17
18
19
C
R
E
B
N
H
20
21
22
23
POWER SOURCE
INTERFACE
24
14
SATELLITE
25
GATEWAY - INTERFACE
RESPONDENT'S MOBILE DEVICE LG V30
OPERATING SYSTEM (OS)
27
WIRELESS/ CELLULAR MODEM
29
26
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
INTERNET WiFi
28
GLOBAL POSITIONING SYSTEM (GPS)
30
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
31
BIOMETRIC FINGERPRINT FACIAL IRIS
32
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
33

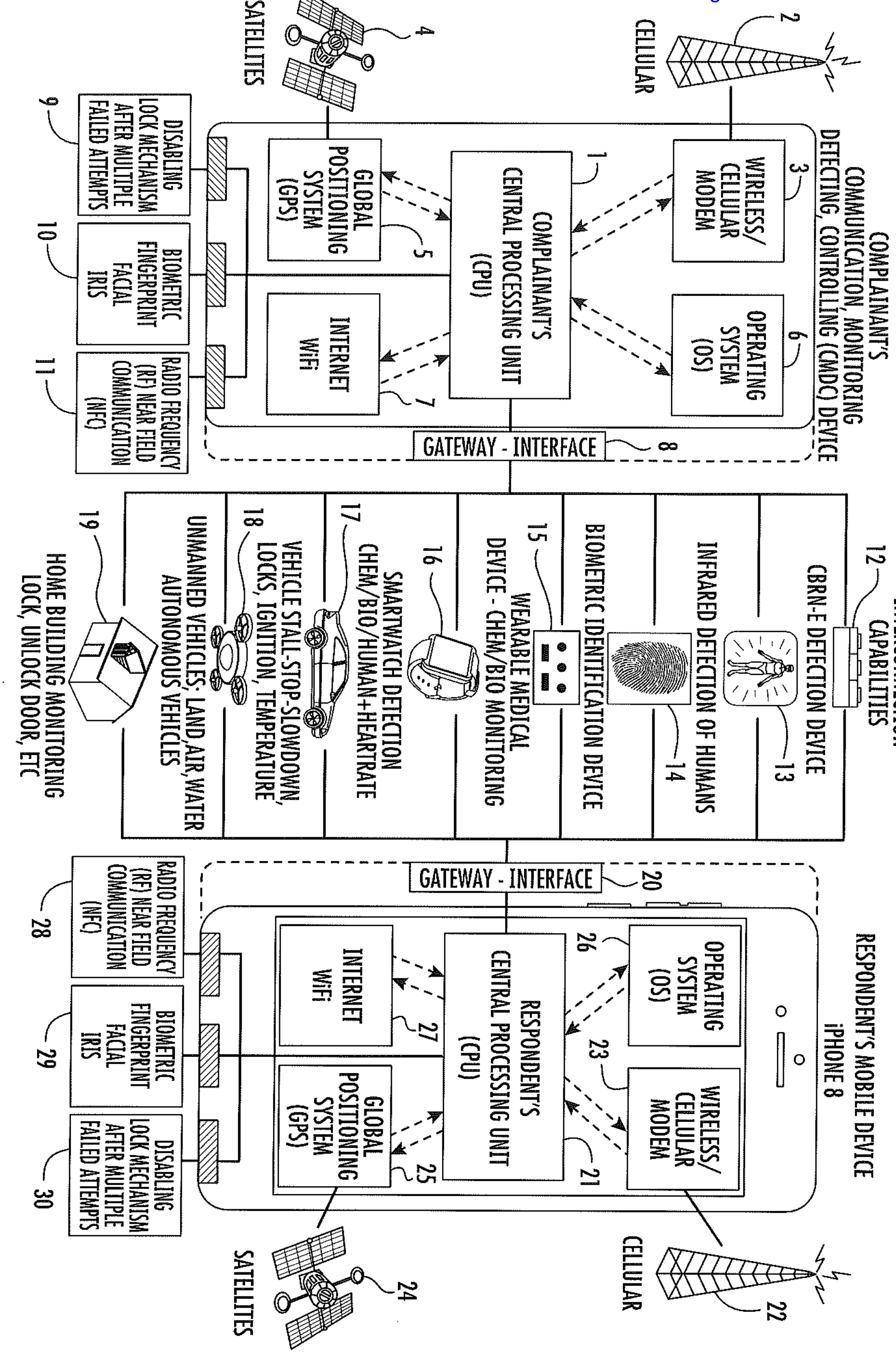

COMPLAINANT'S
COMMUNICATION, MONITORING
DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/
CELLULAR
MODEM
OPERATING
SYSTEM
(OS)
COMPLAINANT'S
CENTRAL PROCESSING UNIT
(CPU)
GLOBAL
POSITIONING
SYSTEM
(GPS)
INTERNET
WiFi
GATEWAY - INTERFACE
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
CELLULAR
CBRNE - H
DETECTION DEVICE:
PLACED IN, ON, UPON OR
ADJACENT THE COMMUNICATION
MONITORING, DETECTING
CONTROLLING (CMDC) DEVICE
LOCATION
CAPABILITY
LOCATION
CAPABILITY
CPU
SENSORS
C
R
E
B
N
H
INTERFACE
INTERFACE
POWER SOURCE
SATELLITE
RESPONDENT'S MOBILE DEVICE
LG G6
OPERATING
SYSTEM
(OS)
WIRELESS/
CELLULAR
MODEM
RESPONDENT'S
CENTRAL PROCESSING UNIT
(CPU)
INTERNET
WiFi
GLOBAL
POSITIONING
SYSTEM
(GPS)
GATEWAY - INTERFACE
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33

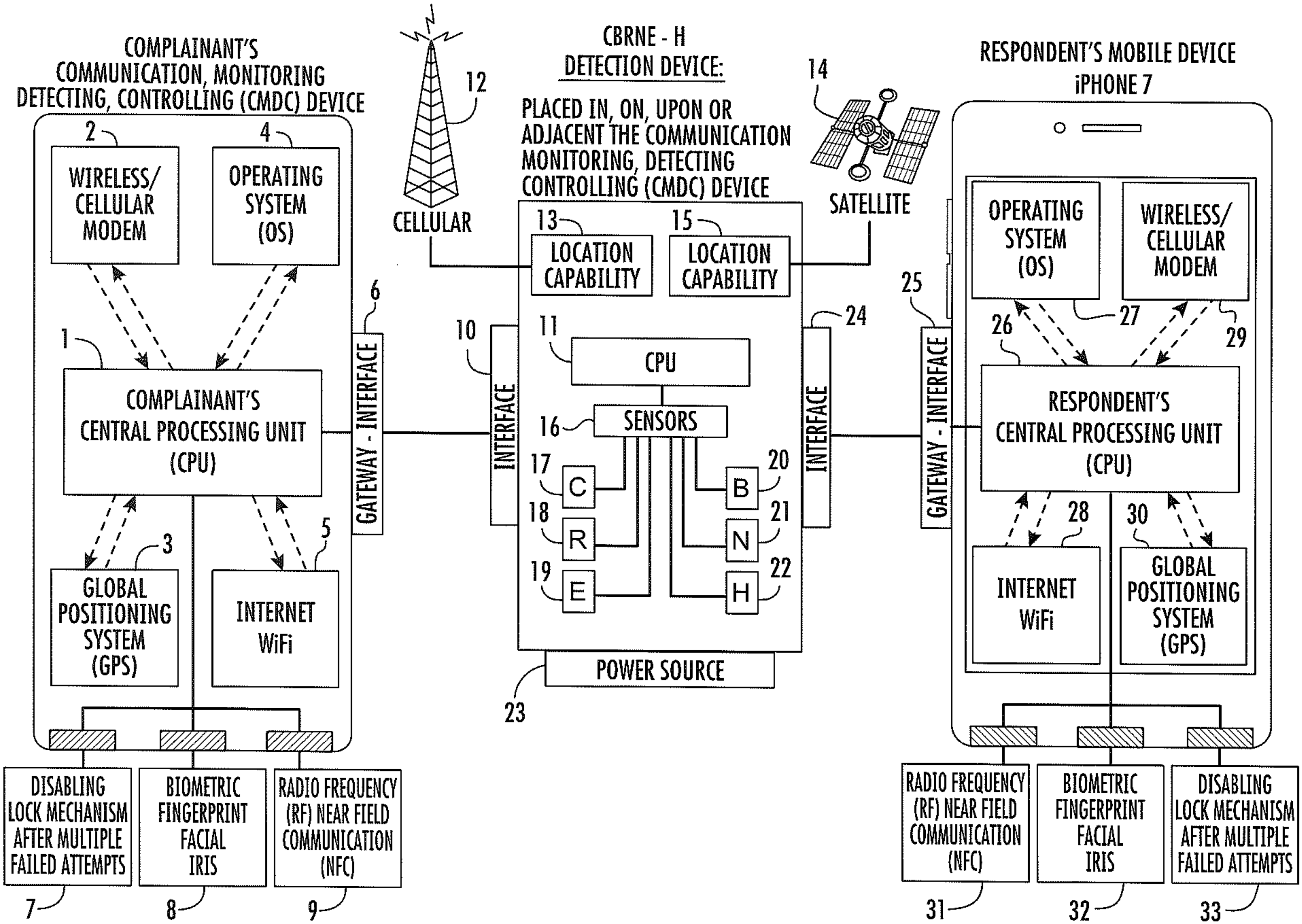

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
OPERATING SYSTEM (OS)
4
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
GATEWAY - INTERFACE
6
INTERFACE
10
NFC
18
OS
16
CPU
11
CELLULAR
13
WiFi
17
GPS
15
CELLULAR
12
CHEM/BIO HEARTRATE SENSORS
19
LG WATCH SPORT
INTERFACE
20
SATELLITE
14
GATEWAY - INTERFACE
21
RESPONDENT'S MOBILE DEVICE LG V30
OPERATING SYSTEM (OS)
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
22
23
INTERNET WiFi
24
WIRELESS/ CELLULAR MODEM
25
GLOBAL POSITIONING SYSTEM (GPS)
26
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
27
BIOMETRIC FINGERPRINT FACIAL IRIS
28
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
29

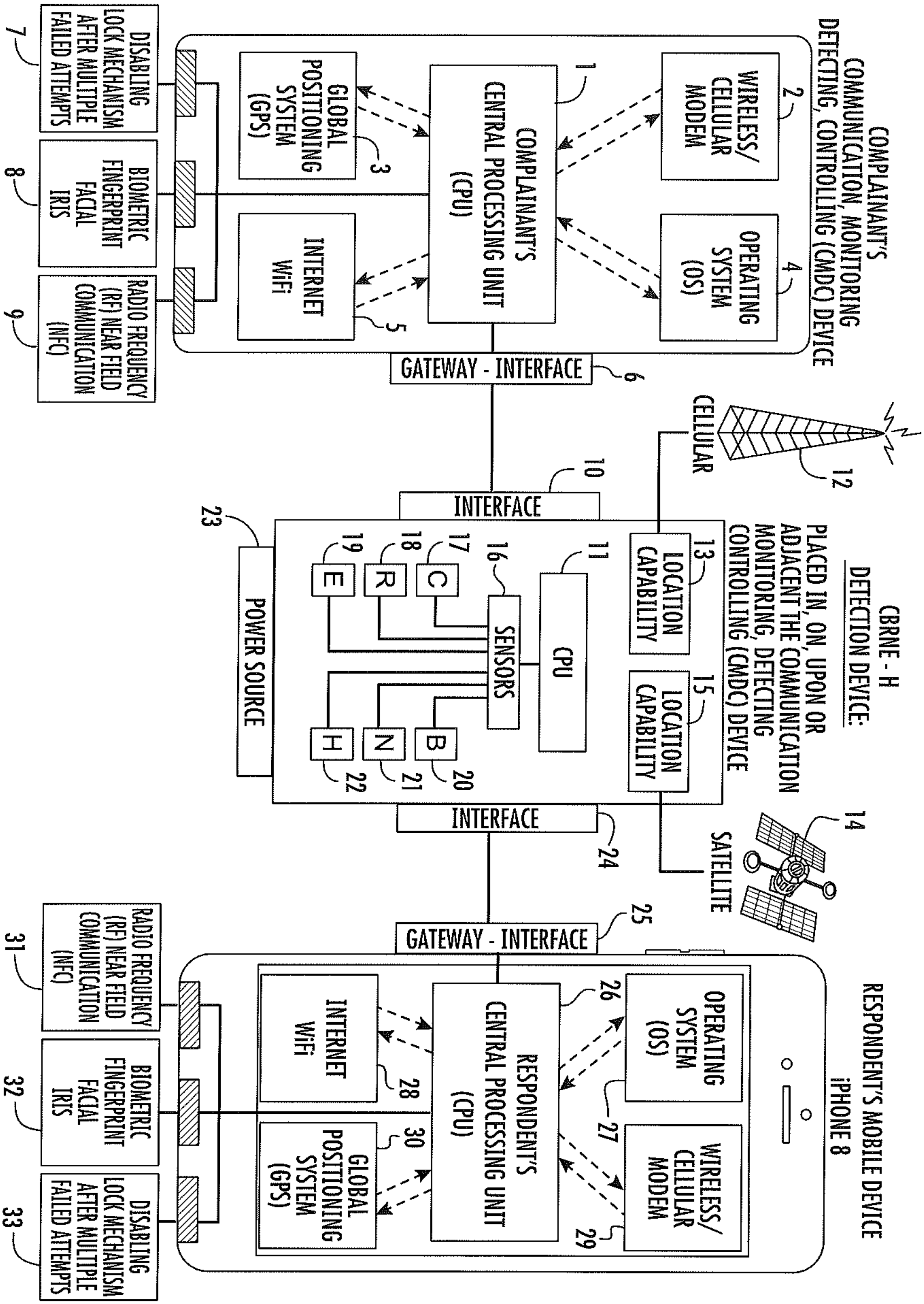

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
1
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
GATEWAY - INTERFACE
6
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
10
INTERFACE
CELLULAR
12
LG WATCH SPORT
NFC
18
OS
16
11
CELLULAR
13
CPU
17
WiFi
GPS
15
19
CHEM/BIO HEARTRATE SENSORS
SATELLITE
14
INTERFACE
20
GATEWAY - INTERFACE
21
RESPONDENT'S MOBILE DEVICE LG G6
OPERATING SYSTEM (OS)
22
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
23
WIRELESS/ CELLULAR MODEM
25
INTERNET WiFi
24
GLOBAL POSITIONING SYSTEM (GPS)
26
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
27
BIOMETRIC FINGERPRINT FACIAL IRIS
28
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
29

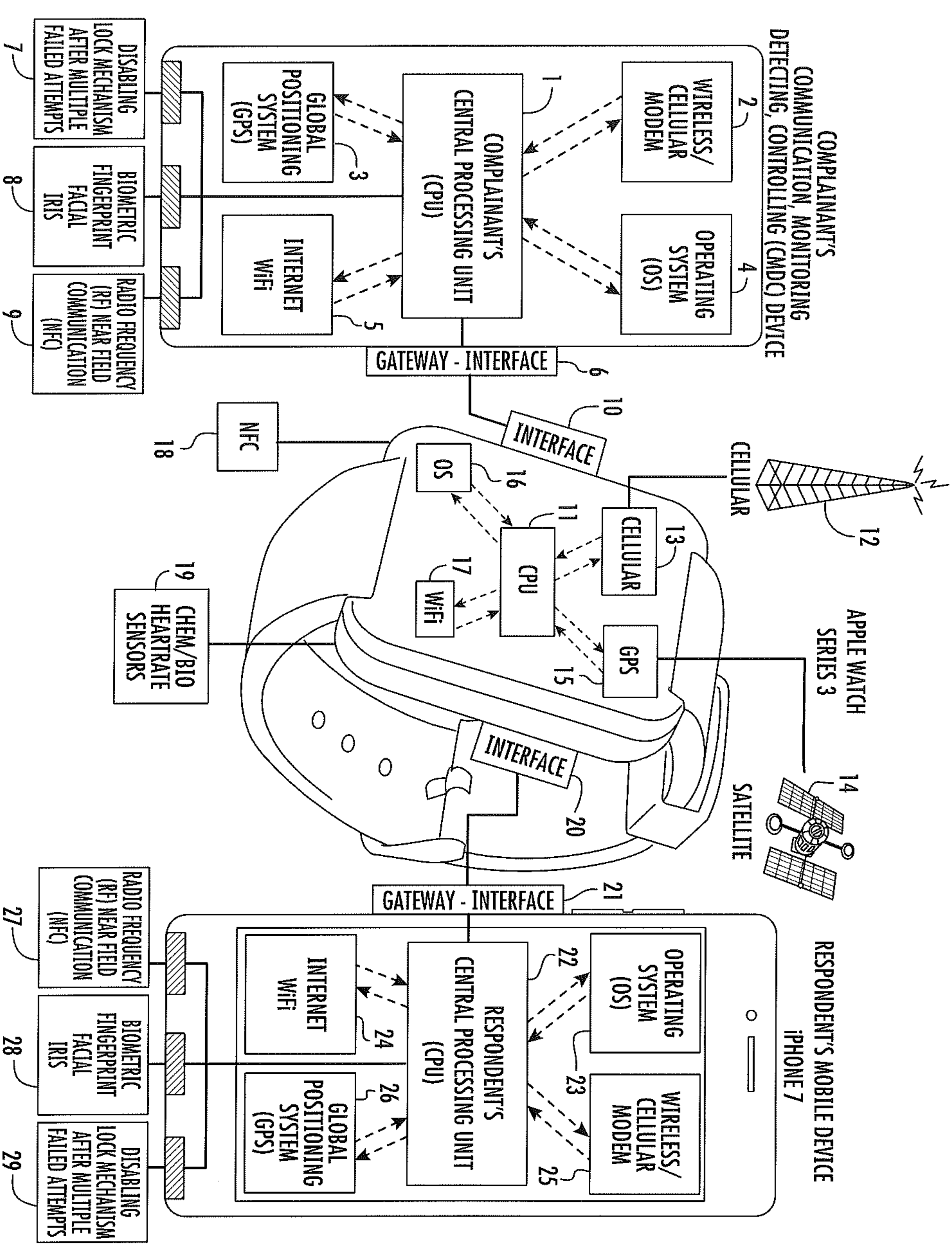
Third Party Government Contractor (Apple Inc.) Utility Specifications and Capabilities for the CMDC Device

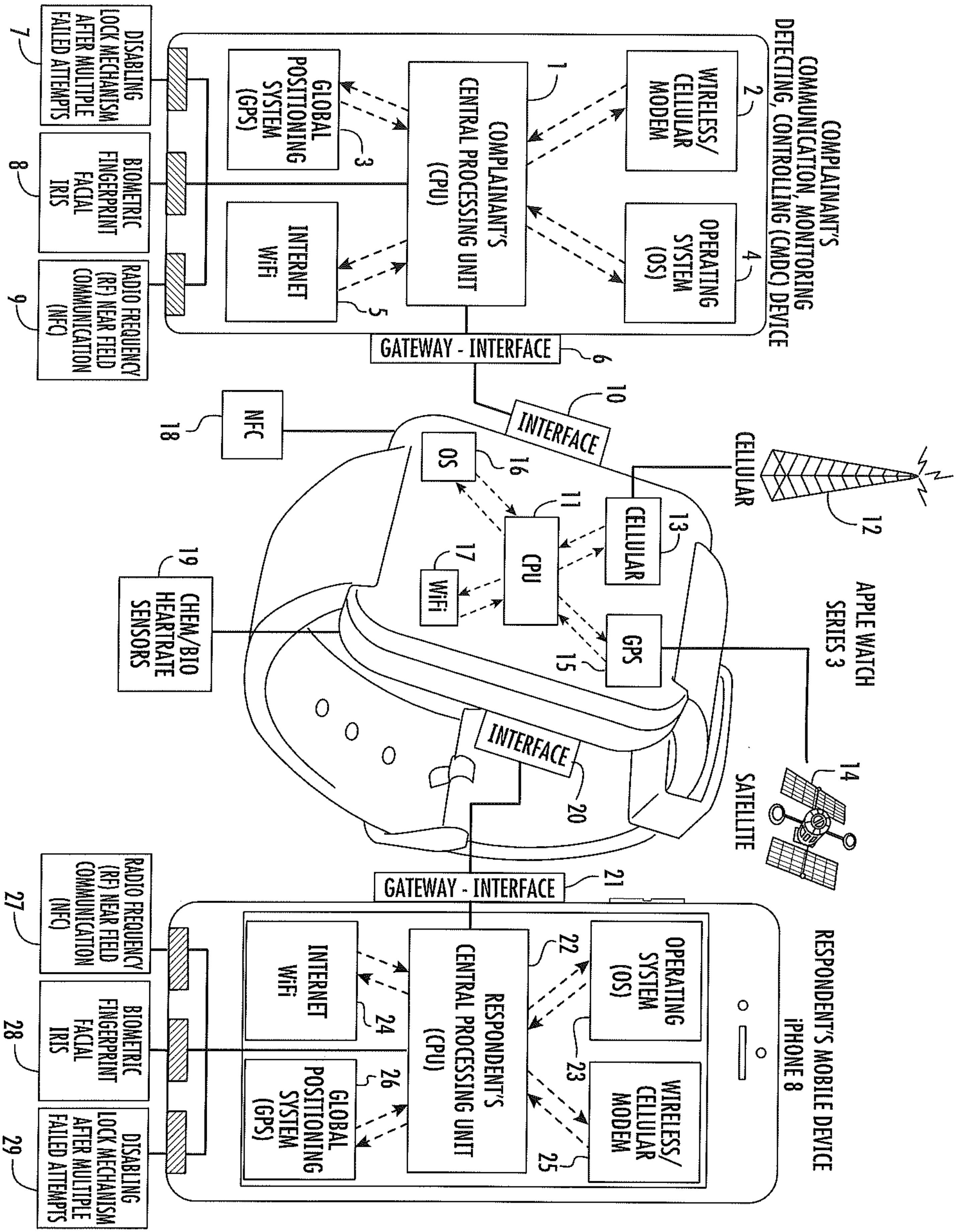

COMPLAINANT'S
COMMUNICATION, MONITORING
DETECTING, CONTROLLING (CMDC) DEVICE
2
CELLULAR
3
WIRELESS/
CELLULAR
MODEM
6
OPERATING
SYSTEM
(OS)
1
COMPLAINANT'S
CENTRAL PROCESSING UNIT
(CPU)
8
GATEWAY - INTERFACE
4
SATELLITES
5
GLOBAL
POSITIONING
SYSTEM
(GPS)
7
INTERNET
WiFi
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
9
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
10
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
11
INTERCONNECTION
CAPABILITIES
12
CBRN-E DETECTION DEVICE
13
INFRARED DETECTION OF HUMANS
14
BIOMETRIC IDENTIFICATION DEVICE
15
WEARABLE MEDICAL
DEVICE - CHEM/BIO MONITORING
16
SMARTWATCH DETECTION
CHEM/BIO/HUMAN+HEARTRATE
17
VEHICLE STALL-STOP-SLOWDOWN,
LOCKS, IGNITION, TEMPERATURE
18
UNMANNED VEHICLES; LAND,AIR,WATER
AUTONOMOUS VEHICLES
19
HOME BUILDING MONITORING
LOCK, UNLOCK DOOR, ETC
RESPONDENT'S MOBILE DEVICE
iPHONE 7
20
GATEWAY - INTERFACE
OPERATING
SYSTEM
(OS)
WIRELESS/
CELLULAR
MODEM
22
CELLULAR
26
23
21
RESPONDENT'S
CENTRAL PROCESSING UNIT
(CPU)
27
25
INTERNET
WiFi
GLOBAL
POSITIONING
SYSTEM
(GPS)
24
SATELLITES
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
28
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
29
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
30


COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
CELLULAR
2
SATELLITES
4
WIRELESS/ CELLULAR MODEM
3
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
5
OPERATING SYSTEM (OS)
6
INTERNET WiFi
7
GATEWAY - INTERFACE
8
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
9
BIOMETRIC FINGERPRINT FACIAL IRIS
10
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
11
INTERCONNECTION CAPABILITIES
12
CBRN-E DETECTION DEVICE
13
INFRARED DETECTION OF HUMANS
14
BIOMETRIC IDENTIFICATION DEVICE
WEARABLE MEDICAL DEVICE - CHEM/BIO MONITORING
15
SMARTWATCH DETECTION CHEM/BIO/HUMAN+HEARTRATE
16
17
VEHICLE STALL-STOP-SLOWDOWN, LOCKS, IGNITION, TEMPERATURE
18
UNMANNED VEHICLES; LAND,AIR,WATER AUTONOMOUS VEHICLES
19
HOME BUILDING MONITORING LOCK, UNLOCK DOOR, ETC
GATEWAY - INTERFACE
20
RESPONDENT'S MOBILE DEVICE iPHONE 8
OPERATING SYSTEM (OS)
26
INTERNET WiFi
27
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
21
23
WIRELESS/ CELLULAR MODEM
GLOBAL POSITIONING SYSTEM (GPS)
25
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
28
BIOMETRIC FINGERPRINT FACIAL IRIS
29
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
30
CELLULAR
22
SATELLITES
24

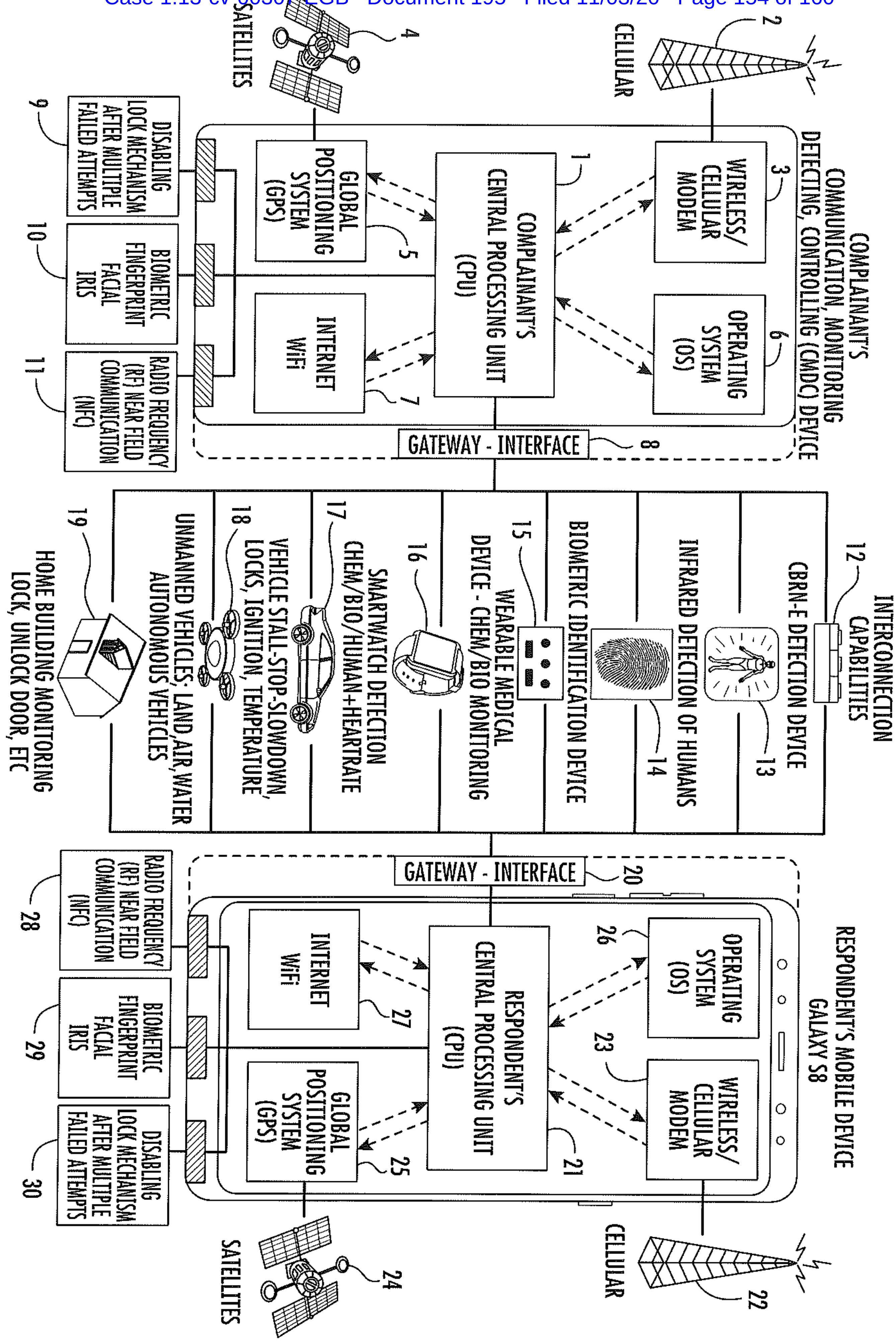

COMPLAINANT'S
COMMUNICATION, MONITORING
DETECTING, CONTROLLING (CMDC) DEVICE
2
WIRELESS/
CELLULAR
MODEM
4
OPERATING
SYSTEM
(OS)
1
COMPLAINANT'S
CENTRAL PROCESSING UNIT
(CPU)
3
GLOBAL
POSITIONING
SYSTEM
(GPS)
5
INTERNET
WiFi
6
GATEWAY - INTERFACE
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
7
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
8
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
9
12
CELLULAR
CBRNE - H
DETECTION DEVICE:
PLACED IN, ON, UPON OR
ADJACENT THE COMMUNICATION
MONITORING, DETECTING
CONTROLLING (CMDC) DEVICE
14
SATELLITE
13
LOCATION
CAPABILITY
15
LOCATION
CAPABILITY
10
INTERFACE
11
CPU
16
SENSORS
17
C
18
R
19
E
20
B
21
N
22
H
24
INTERFACE
POWER SOURCE
23
RESPONDENT'S MOBILE DEVICE
iPHONE 7
25
GATEWAY - INTERFACE
OPERATING
SYSTEM
(OS)
WIRELESS/
CELLULAR
MODEM
26
27
29
RESPONDENT'S
CENTRAL PROCESSING UNIT
(CPU)
28
30
INTERNET
WiFi
GLOBAL
POSITIONING
SYSTEM
(GPS)
RADIO FREQUENCY
(RF) NEAR FIELD
COMMUNICATION
(NFC)
31
BIOMETRIC
FINGERPRINT
FACIAL
IRIS
32
DISABLING
LOCK MECHANISM
AFTER MULTIPLE
FAILED ATTEMPTS
33

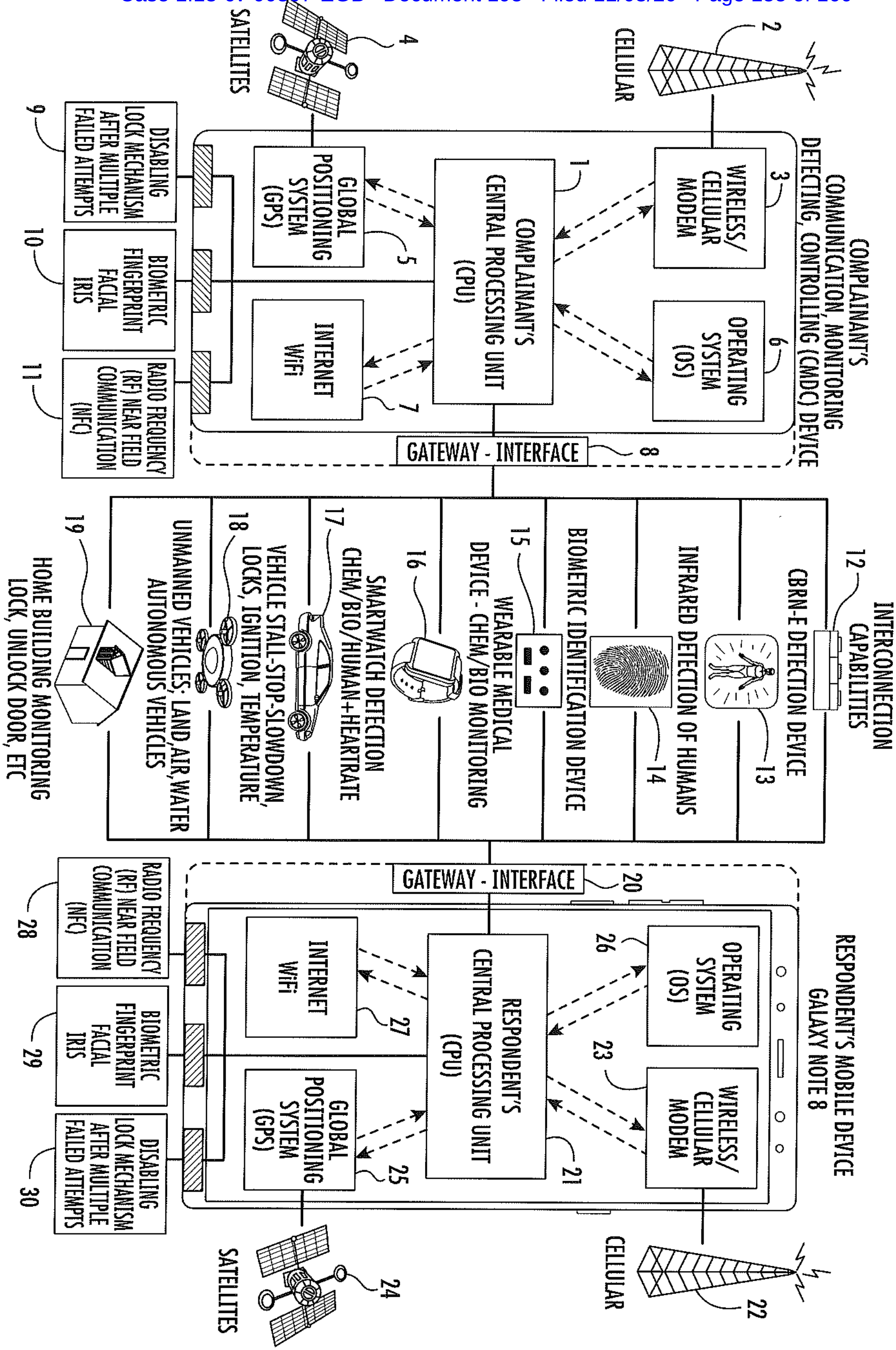

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
GATEWAY - INTERFACE
6
CELLULAR
12
INTERFACE
10
CBRNE - H DETECTION DEVICE: PLACED IN, ON, UPON OR ADJACENT THE COMMUNICATION MONITORING, DETECTING CONTROLLING (CMDC) DEVICE
LOCATION CAPABILITY
13
LOCATION CAPABILITY
15
CPU
11
SENSORS
16
C
17
R
18
E
19
B
20
N
21
H
22
POWER SOURCE
23
INTERFACE
24
SATELLITE
14
GATEWAY - INTERFACE
25
RESPONDENT'S MOBILE DEVICE iPHONE 8
OPERATING SYSTEM (OS)
27
WIRELESS/ CELLULAR MODEM
29
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
26
INTERNET WiFi
28
GLOBAL POSITIONING SYSTEM (GPS)
30
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
31
BIOMETRIC FINGERPRINT FACIAL IRIS
32
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
33

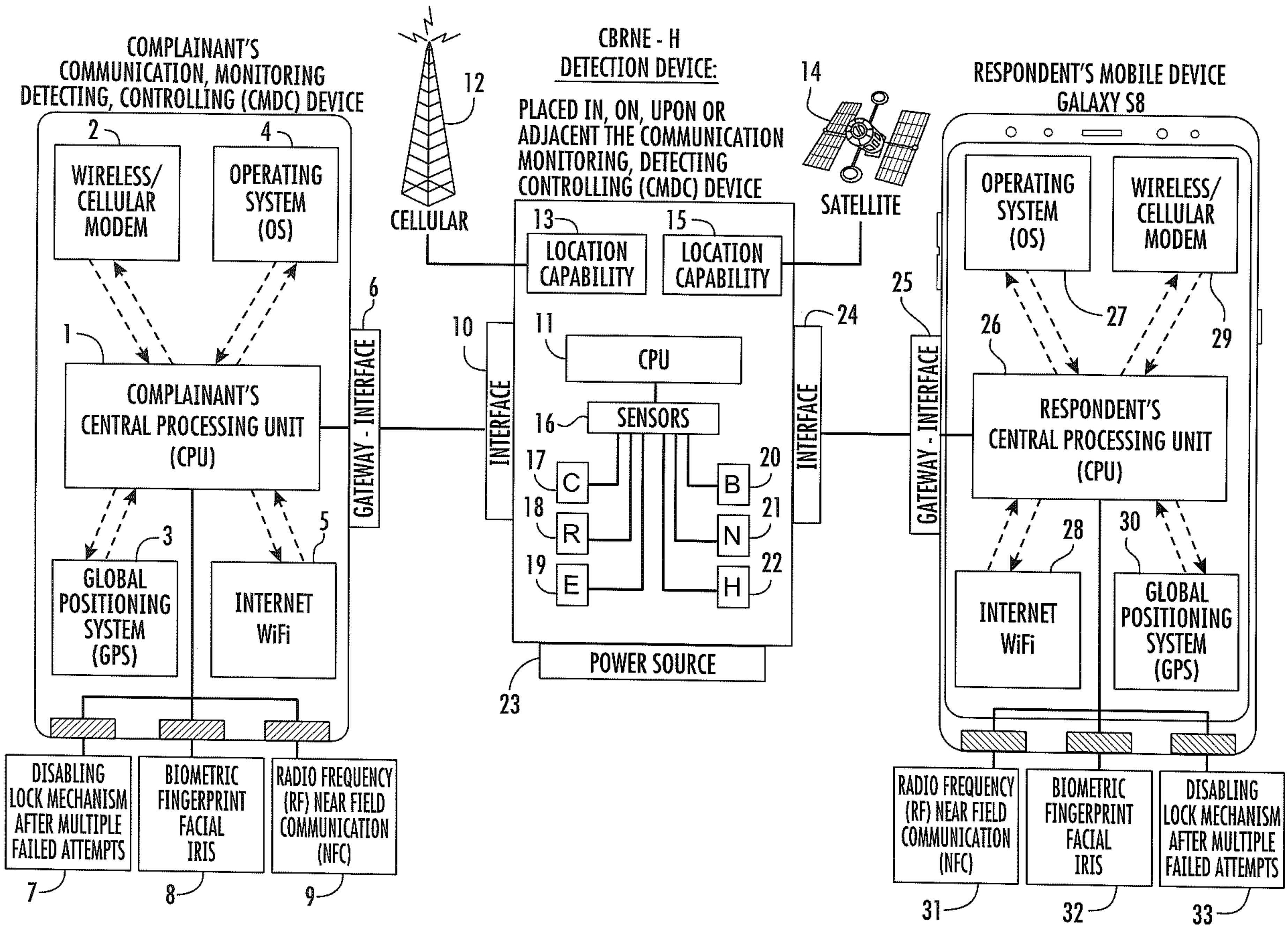

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
GATEWAY - INTERFACE
6
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
INTERFACE
10
CELLULAR
12
NFC
18
OS
16
CPU
11
CELLULAR
13
WiFi
17
GPS
15
APPLE WATCH SERIES 3
CHEM/BIO HEARTRATE SENSORS
19
INTERFACE
20
SATELLITE
14
GATEWAY - INTERFACE
21
RESPONDENT'S MOBILE DEVICE iPHONE 7
OPERATING SYSTEM (OS)
23
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
22
WIRELESS/ CELLULAR MODEM
25
INTERNET WiFi
24
GLOBAL POSITIONING SYSTEM (GPS)
26
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
27
BIOMETRIC FINGERPRINT FACIAL IRIS
28
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
29

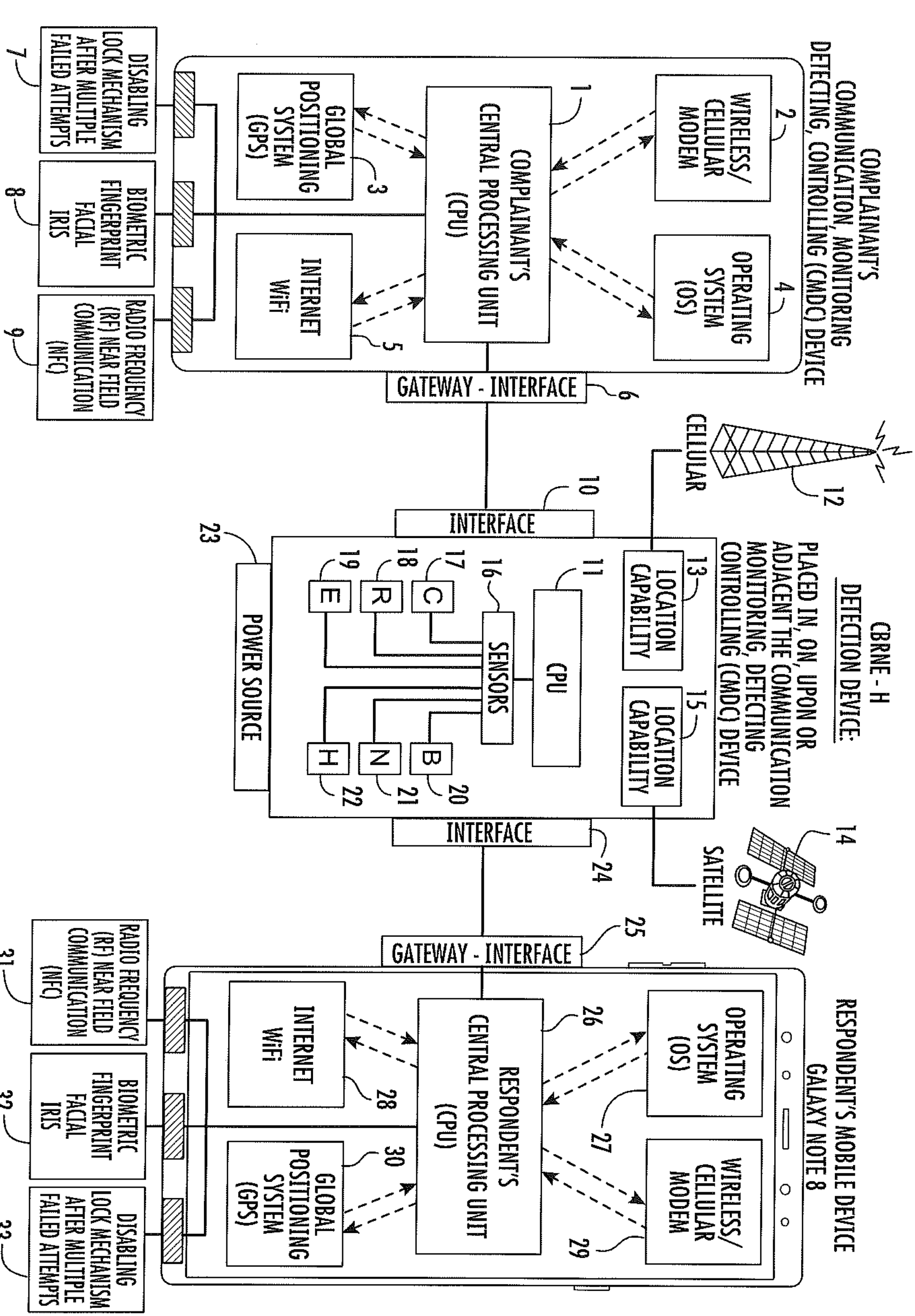

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
GATEWAY - INTERFACE
6
INTERFACE
10
NFC
18
CELLULAR
12
OS
16
CPU
11
CELLULAR
13
WiFi
17
GPS
15
APPLE WATCH SERIES 3
CHEM/BIO HEARTRATE SENSORS
19
INTERFACE
20
SATELLITE
14
GATEWAY - INTERFACE
21
RESPONDENT'S MOBILE DEVICE iPHONE 8
OPERATING SYSTEM (OS)
22
23
WIRELESS/ CELLULAR MODEM
25
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
INTERNET WiFi
24
GLOBAL POSITIONING SYSTEM (GPS)
26
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
27
BIOMETRIC FINGERPRINT FACIAL IRIS
28
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
29

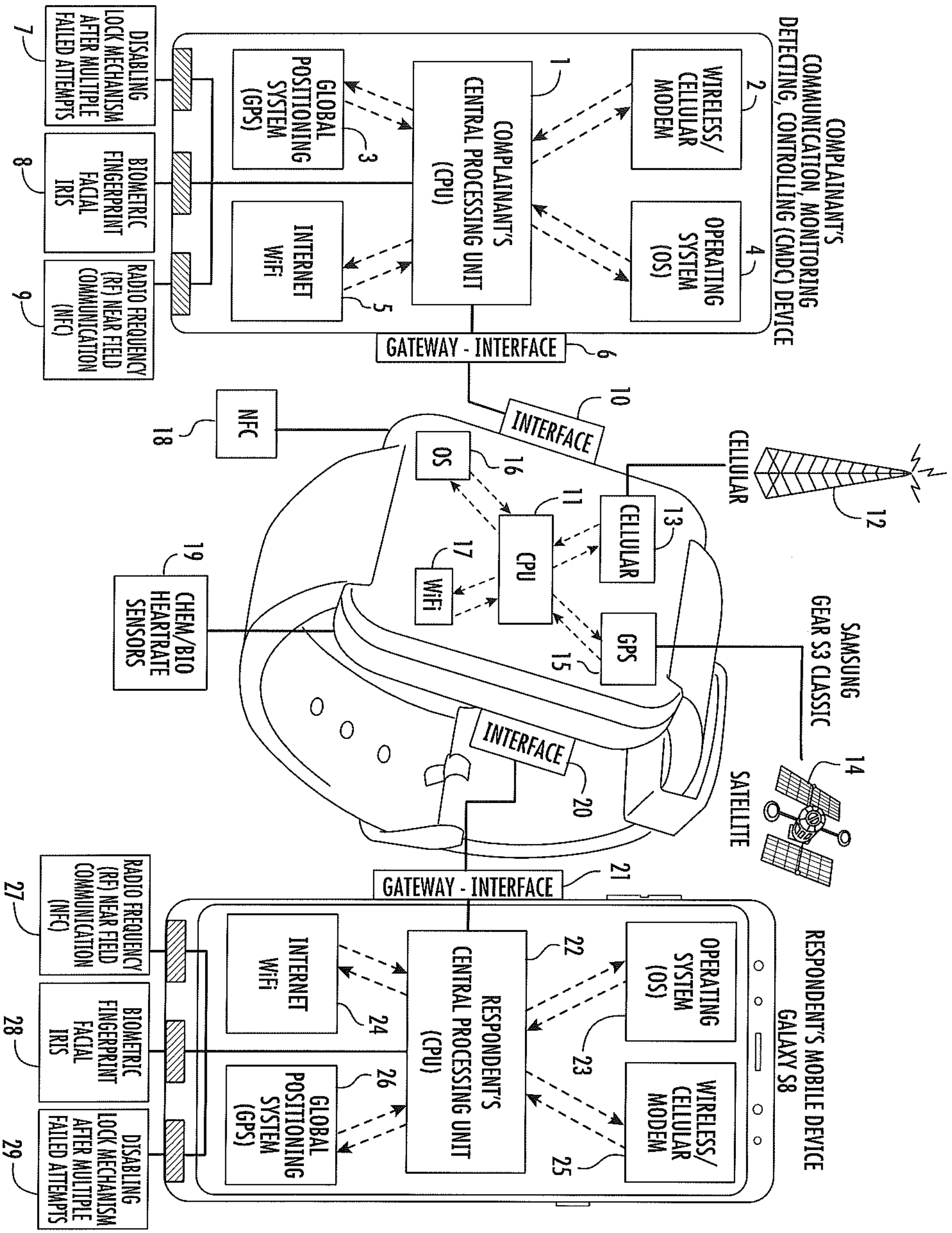
Third Party Government Contractor (Apple Inc.) Utility Specifications and Capabilities for the CMDC Device

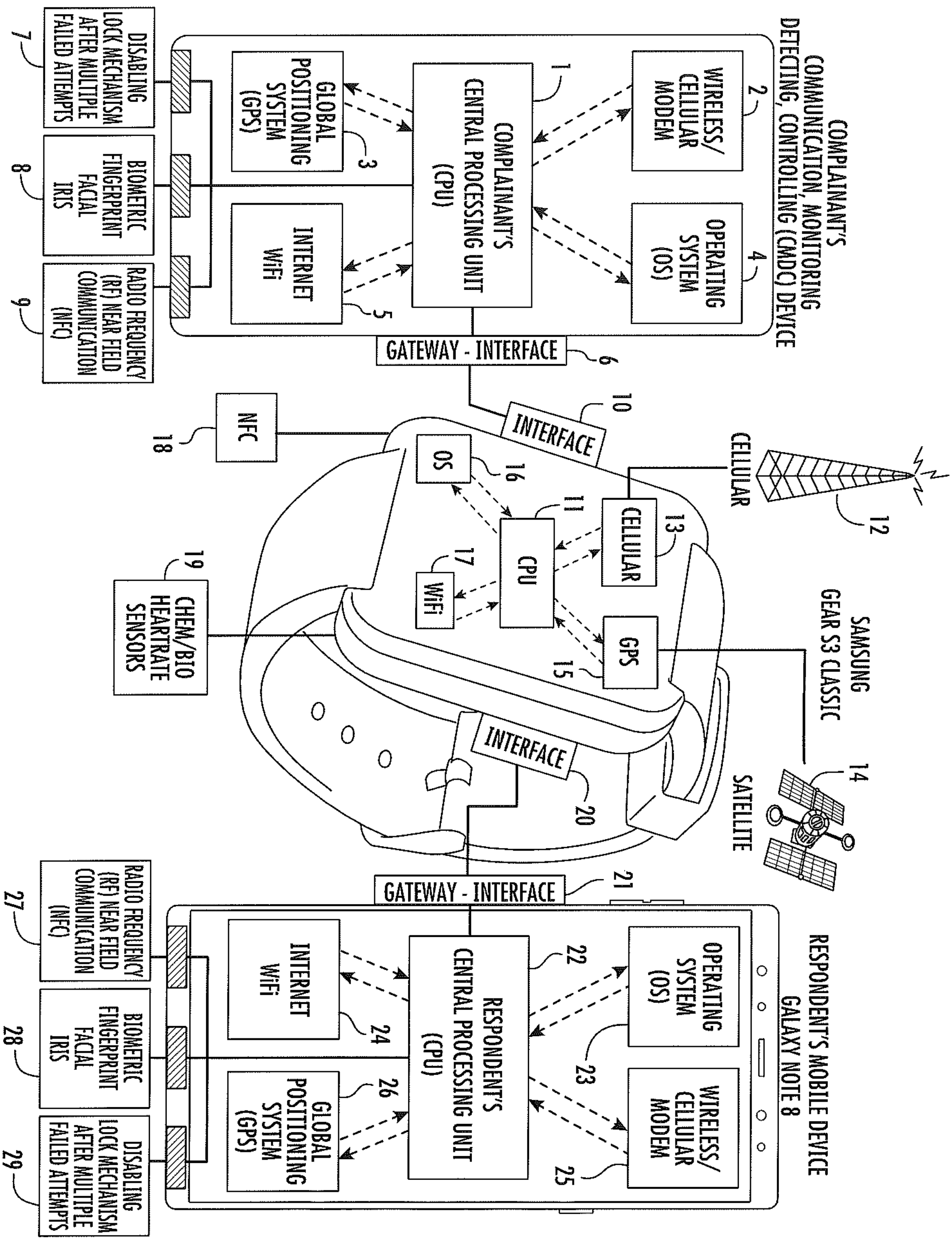

COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
CELLULAR
2
SATELLITES
4
WIRELESS/ CELLULAR MODEM
3
OPERATING SYSTEM (OS)
6
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
5
INTERNET WiFi
7
GATEWAY - INTERFACE
8
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
9
BIOMETRIC FINGERPRINT FACIAL IRIS
10
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
11
INTERCONNECTION CAPABILITIES
12
CBRN-E DETECTION DEVICE
13
INFRARED DETECTION OF HUMANS
14
BIOMETRIC IDENTIFICATION DEVICE
WEARABLE MEDICAL DEVICE - CHEM/BIO MONITORING
15
SMARTWATCH DETECTION CHEM/BIO/HUMAN+HEARTRATE
16
VEHICLE STALL-STOP-SLOWDOWN, LOCKS, IGNITION, TEMPERATURE
17
UNMANNED VEHICLES; LAND,AIR,WATER AUTONOMOUS VEHICLES
18
HOME BUILDING MONITORING LOCK, UNLOCK DOOR, ETC
19
GATEWAY - INTERFACE
20
RESPONDENT'S MOBILE DEVICE GALAXY S8
OPERATING SYSTEM (OS)
26
WIRELESS/ CELLULAR MODEM
23
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
21
INTERNET WiFi
27
GLOBAL POSITIONING SYSTEM (GPS)
25
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
28
BIOMETRIC FINGERPRINT FACIAL IRIS
29
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
30
CELLULAR
22
SATELLITES
24


COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
CELLULAR
2
SATELLITES
4
WIRELESS/ CELLULAR MODEM
3
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
OPERATING SYSTEM (OS)
6
GLOBAL POSITIONING SYSTEM (GPS)
5
INTERNET WiFi
7
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
9
BIOMETRIC FINGERPRINT FACIAL IRIS
10
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
11
GATEWAY - INTERFACE
8
INTERCONNECTION CAPABILITIES
12
CBRN-E DETECTION DEVICE
13
INFRARED DETECTION OF HUMANS
14
BIOMETRIC IDENTIFICATION DEVICE
15
WEARABLE MEDICAL DEVICE - CHEM/BIO MONITORING
16
SMARTWATCH DETECTION CHEM/BIO/HUMAN+HEARTRATE
17
VEHICLE STALL-STOP-SLOWDOWN, LOCKS, IGNITION, TEMPERATURE
18
UNMANNED VEHICLES; LAND,AIR,WATER AUTONOMOUS VEHICLES
19
HOME BUILDING MONITORING LOCK, UNLOCK DOOR, ETC
GATEWAY - INTERFACE
20
RESPONDENT'S MOBILE DEVICE GALAXY NOTE 8
OPERATING SYSTEM (OS)
26
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
21
WIRELESS/ CELLULAR MODEM
23
INTERNET WiFi
27
GLOBAL POSITIONING SYSTEM (GPS)
25
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
28
BIOMETRIC FINGERPRINT FACIAL IRIS
29
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
30
CELLULAR
22
SATELLITES
24


COMPLAINANT'S
COMMUNICATION, MONITORING
DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
OPERATING SYSTEM (OS)
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
GLOBAL POSITIONING SYSTEM (GPS)
INTERNET WiFi
GATEWAY - INTERFACE
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
BIOMETRIC FINGERPRINT FACIAL IRIS
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
CELLULAR
CBRNE - H
DETECTION DEVICE:
PLACED IN, ON, UPON OR ADJACENT THE COMMUNICATION MONITORING, DETECTING CONTROLLING (CMDC) DEVICE
LOCATION CAPABILITY
LOCATION CAPABILITY
INTERFACE
CPU
SENSORS
C
R
E
B
N
H
INTERFACE
POWER SOURCE
SATELLITE
RESPONDENT'S MOBILE DEVICE
GALAXY S8
OPERATING SYSTEM (OS)
WIRELESS/ CELLULAR MODEM
GATEWAY - INTERFACE
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
INTERNET WiFi
GLOBAL POSITIONING SYSTEM (GPS)
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
BIOMETRIC FINGERPRINT FACIAL IRIS
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33


COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
GATEWAY - INTERFACE
6
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
CELLULAR
12
INTERFACE
10
CBRNE - H DETECTION DEVICE:
PLACED IN, ON, UPON OR ADJACENT THE COMMUNICATION MONITORING, DETECTING CONTROLLING (CMDC) DEVICE
LOCATION CAPABILITY
13
LOCATION CAPABILITY
15
CPU
11
SENSORS
16
C
17
R
18
E
19
B
20
N
21
H
22
POWER SOURCE
23
INTERFACE
24
SATELLITE
14
GATEWAY - INTERFACE
25
RESPONDENT'S MOBILE DEVICE GALAXY NOTE 8
OPERATING SYSTEM (OS)
27
WIRELESS/ CELLULAR MODEM
29
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
26
INTERNET WiFi
28
GLOBAL POSITIONING SYSTEM (GPS)
30
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
31
BIOMETRIC FINGERPRINT FACIAL IRIS
32
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
33


COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
1
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
OPERATING SYSTEM (OS)
4
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
GATEWAY - INTERFACE
6
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
10
INTERFACE
CELLULAR
12
NFC
18
OS
16
11
CELLULAR
13
CPU
17
WiFi
GPS
15
SAMSUNG GEAR S3 CLASSIC
CHEM/BIO HEARTRATE SENSORS
19
INTERFACE
20
14
SATELLITE
GATEWAY - INTERFACE
21
RESPONDENT'S MOBILE DEVICE GALAXY S8
OPERATING SYSTEM (OS)
22
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
INTERNET WiFi
24
23
WIRELESS/ CELLULAR MODEM
25
GLOBAL POSITIONING SYSTEM (GPS)
26
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
27
BIOMETRIC FINGERPRINT FACIAL IRIS
28
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
29


COMPLAINANT'S COMMUNICATION, MONITORING DETECTING, CONTROLLING (CMDC) DEVICE
WIRELESS/ CELLULAR MODEM
2
OPERATING SYSTEM (OS)
4
COMPLAINANT'S CENTRAL PROCESSING UNIT (CPU)
1
GLOBAL POSITIONING SYSTEM (GPS)
3
INTERNET WiFi
5
GATEWAY - INTERFACE
6
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
7
BIOMETRIC FINGERPRINT FACIAL IRIS
8
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
9
INTERFACE
10
CELLULAR
12
OS
16
CPU
11
CELLULAR
13
WiFi
17
GPS
15
NFC
18
CHEM/BIO HEARTRATE SENSORS
19
SAMSUNG GEAR S3 CLASSIC
SATELLITE
14
INTERFACE
20
GATEWAY - INTERFACE
21
RESPONDENT'S MOBILE DEVICE GALAXY NOTE 8
OPERATING SYSTEM (OS)
23
WIRELESS/ CELLULAR MODEM
25
RESPONDENT'S CENTRAL PROCESSING UNIT (CPU)
22
INTERNET WiFi
24
GLOBAL POSITIONING SYSTEM (GPS)
26
RADIO FREQUENCY (RF) NEAR FIELD COMMUNICATION (NFC)
27
BIOMETRIC FINGERPRINT FACIAL IRIS
28
DISABLING LOCK MECHANISM AFTER MULTIPLE FAILED ATTEMPTS
29

EXPRESS MAIL
UNITED STATES POSTAL SERVICE®

AFFIX P
CORPO
LABEL

U.S. POSTAGE PAID
PME 1-Day
GREENVILLE, SC
29606
JUL 06, 20
AMOUNT
$39.55
R2303S103999-09

UNITED STATES POSTAL SERVICE®
1007
20439

Y URGENT Please Rush To Addressee

EXPRESS MAIL
UNITED STATES POSTAL SERVICE™
www.usps.gov
LABEL 119

urgentemente

FOR PICKUP OR TRACKING CALL 1
, llame al 1

WRITE FIRMLY WITH BALL POINT PEN ON HARD SURFACE TO MAKE ALL COPIES LEGIBLE.

CUSTOMER USE ONLY

FROM: (PLEASE PRINT) PHONE (864) 288-5605
LARRY GOLDEN
740 WOODRUFF RD.
#1102
GREENVILLE, SC 29607

EL 098099143 US

UNITED STATES POSTAL SERVICE®
PRIORITY ★ MAIL ★ EXPRESS™

RECEIVED
JUL - 9 2020
OFFICE OF THE CLERK
U.S. COURT OF FEDERAL CLAIMS

PAYMENT BY ACCOUNT (if applicable)
USPS® Corporate Acct. No.
Federal Agency Acct. No. or Postal Service™ Acct. No.

DELIVERY OPTIONS (Customer Use Only)
☒ **SIGNATURE REQUIRED** *Note:* The mailer must check the "Signature Required" box if the mailer: 1) Requires the addressee's signature; OR 2) Purchases additional insurance; OR 3) Purchases COD service; OR 4) Purchases Return Receipt service. If the box is not checked, the Postal Service will leave the item in the addressee's mail receptacle or other secure location without attempting to obtain the addressee's signature on delivery.
Delivery Options
☐ No Saturday Delivery (delivered next business day)
☐ Sunday/Holiday Delivery Required (additional fee, where available*)
☐ 10:30 AM Delivery Required (additional fee, where available*)
*Refer to USPS.com® or local Post Office™ for availability.

TO: (PLEASE PRINT) PHONE ( )
UNITED STATES COURT OF FEDERAL CLAIMS
CASE No: 13-307C
JUDGE ERIC G. BRUGGINK
HOWARD T. MARKEY NATIONAL COURTS BUILDING
717 MADISON PLACE, NW
WASHINGTON, DC
ZIP + 4® (U.S. ADDRESSES ONLY)
2 0 4 3 9 - _ _ _ _

■ For pickup or USPS Tracking™, visit USPS.com or call 800-222-1811.
■ $100.00 insurance included.

ORIGIN (POSTAL SERVICE USE ONLY)

☒ 1-Day	☐ 2-Day	☐ Military	☐ DPO
PO ZIP Code: 29606	Scheduled Delivery Date (MM/DD/YY): 070720	Postage: $ 39.55	
Date Accepted (MM/DD/YY): 070620	Scheduled Delivery Time: ☐ 10:30 AM ☐ 3:00 PM ☐ 12 NOON	Insurance Fee: $	COD Fee: $
Time Accepted: 1009 ☒ AM ☐ PM	10:30 AM Delivery Fee: $	Return Receipt Fee: $	Live Animal Transportation Fee: $
Weight: 2 lbs. 7 ozs. ☐ Flat Rate	Sunday/Holiday Premium Fee: $	Total Postage & Fees: $ 39.55	
	Acceptance Employee Initials: MW		

RECEIVED
JUL - 7 2020
OFFICE OF THE CLERK
U.S. COURT OF FEDERAL CLAIMS

DELIVERY (POSTAL SERVICE USE ONLY)

Delivery Attempt (MM/DD/YY)	Time	Employee Signature
	☐ AM ☐ PM	
	☐ AM ☐ PM	

LABEL 11-B, SEPTEMBER 2015 PSN 7690-02-000-9996 1-ORIGIN POST OFFICE COPY

block (blue area
erida en la secc
upper right h
nt number on l
a indicada en
bierno, escrib
structions. B
retain for yo
as instruccio
te posterior
service (O
ss Mail pa

Llame al 1-8 otro servicio de recole
EXPRESS